INSPECTOR GENERAL
U.S. Department of Defense

Management Challenges

Fiscal Year 2016

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

For more information about whistleblower protection, please see the inside back cover.

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

TOP MANAGEMENT AND PERFORMANCE CHALLENGES FACING THE DEPARTMENT OF DEFENSE

Public Law 106-531, the "Reports Consolidation Act of 2000," requires that Inspectors General prepare an annual statement that summarizes what they consider to be the "most serious management and performance challenges facing the agency." By statute, this statement is required to be included in the Department's Agency Financial Report.

The following is the Department of Defense Office of Inspector General's (DoD OIG) statement regarding the top management and performance challenges facing the DoD. The DoD OIG identified these challenges based on DoD OIG oversight work, research, and judgment; oversight work done by other components within the DoD; and oversight projects by the Government Accountability Office. While we reviewed DoD statements, documents, and assessments of the critical issues it faces, we identified these challenges independently.

In this report, we summarize each challenge, outline steps that the DoD has taken to address the challenge, and discuss ongoing future oversight work related to the challenge. The ten challenges are not necessarily placed in order of importance; rather, they are all critical and difficult management and performance challenges facing the DoD.

The top ten challenges are:

1. Countering Global Strategic Challenges
2. Countering the Terrorist Threat
3. Enabling Effective Acquisition and Contract Management
4. Increasing Cyber Security and Cyber Capabilities
5. Improving Financial Management
6. Protecting Key Defense Infrastructure
7. Developing Full Spectrum Total Force Capabilities
8. Building and Maintaining Force Readiness
9. Ensuring Ethical Conduct
10. Promoting Continuity and Effective Transition Management

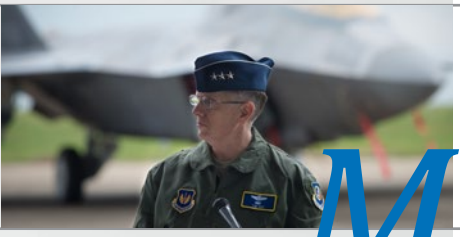
The OIG looks forward to working with the DoD to continually improve the DoD's efforts to address these important challenges.

Glenn A. Fine
Acting Inspector General

THROUGH THE LENS

Photojournalists and broadcast journalists document base operations for historical and investigative purposes.

Photo courtesy of U.S. Air Force, Airman 1st Class Christopher Maldonado



Management Challenges

Fiscal Year 2016

Content

COUNTERING GLOBAL STRATEGIC CHALLENGES

Interagency cooperation is fundamental to countering global threats.

the Challenge—#1

Countering Global Strategic Challenges

Evolving global threats are a top challenge for the DoD. Secretary of Defense Carter has identified the five most significant global strategic challenges to U.S. interests as Russia, China, North Korea, Iran, and terrorism. In a speech at a Center for New American Security conference on March 17, 2016, The Secretary stated that these threats require new ways of planning, budgeting, and operating. He noted that the DoD must have the capability to staff, equip, and deploy personnel and equipment to combat multiple challenges throughout the world.

Maintaining a level of preparedness to address multiple global threats poses major management challenges for the DoD.

CARGO DELIVERY

USS Bonhomme Richard is operating in the South China Sea in support of security and stability in the Indo-Asia Pacifice region.

Photo by U.S. Navy, Petty Officer 2nd Class Diana Quinlan/Released

Global Threats

As the Secretary stated in his testimony to the Senate Armed Services Committee on September 22, 2016, "We don't have the luxury of choosing between these challenges, which is why American soldiers, sailors, airmen, and Marines are working with partners from our worldwide coalition in more ways and with more power every day."

With regard to the challenge from China, the 2017 Defense Posture Statement reported that the specific U.S. objective in Asia and the Pacific is "maintaining freedom of navigation and overflight, full and unimpeded lawful commerce, and that disputes are resolved peacefully." To accomplish this, he said, "the United States will continue to fly, sail, and operate wherever international law allows."

However, in recent years, China has undertaken aggressive and expansionist reclamation activities in the South China Sea and East China Sea. By creating artificial islands in maritime territory claimed by multiple neighboring countries, China has increased regional tensions and presented a significant challenge to U.S. interests in the region. Additionally, China has been building and improving its military capabilities, such as nuclear

weapons, ballistic and cruise missiles, counter-space and offensive cyber capabilities, electronic warfare systems, a stronger, more lethal surface and submarine warfare capability, and a more sophisticated air force.

At a June 2016 conference, the Secretary stated, "Although we have disagreements with China, especially over its destabilizing behavior in the South China Sea, we're committed to working with them and to persuade them to avoid self-isolation. That is one reason why we'll continue to pursue a stronger, bilateral military-to-military relationship with our colleagues in China." The Secretary also emphasized the importance of maintaining trilateral and multilateral country relationships in the Asia-Pacific region in support of U.S. strategic interests.

Similarly, the Chief of Naval Operations at the same conference noted that the United States has many strong bilateral relationships in the Pacific but that increasing trilateral and multilateral collaboration is key to maintaining regional stability.

In addition to security challenges in the Pacific region posed by China, North Korea and its pursuit of nuclear weapons and ballistic missile technologies, and its role in their proliferation, presents a growing strategic threat. North Korea directly threatens its neighbors, South Korea and Japan, with which the United States has security treaty commitments. Moreover, North Korean leaders regularly assert that the United States is its principal enemy.

DoD is working to develop a comprehensive set of alliance capabilities to counter the growing North Korean ballistic missile threat.

According to the Secretary in the 2016 Defense Posture Statement, the DoD is working to develop a comprehensive set of alliance capabilities to counter the growing North Korean ballistic missile threat. In that regard, the United States and South Korea jointly announced consultations concerning the feasibility of deploying a Terminal High-Altitude Area Defense system to the Korean peninsula. The United States currently maintains a significant ground, air, and sea force based in South Korea and Japan to deter North Korean aggression. Any aggression by North Korea against the security of South Korea or Japan could require a U.S. response and appropriate action by DoD and its U.S. Forces Korea command.

According to the Secretary's 2017 Defense Posture statement, Russia's increasingly aggressive posture in Europe poses major challenges. The posture statement notes that "Russia has in recent years appeared intent to erode the principled international order that has served us, our friends and allies, the international community, and also Russia itself so well for

so long." Russia has violated the sovereignty of the Ukraine, Moldova, and Georgia, and it actively seeks to intimidate its Baltic neighbors. In addition to seizing the Crimea, sovereign territory of the Ukraine, Russia has deployed a significant military force to the eastern Ukraine and continues to threaten to destabilize the rest of the country. Its tactics range from the use of media manipulation, support for right-wing political parties, cyber weapons that can disrupt critical infrastructure, and hostile intervention by Russian military aircraft flown dangerously close to ships and aircraft from the U.S. and North Atlantic Treaty Organization (NATO).

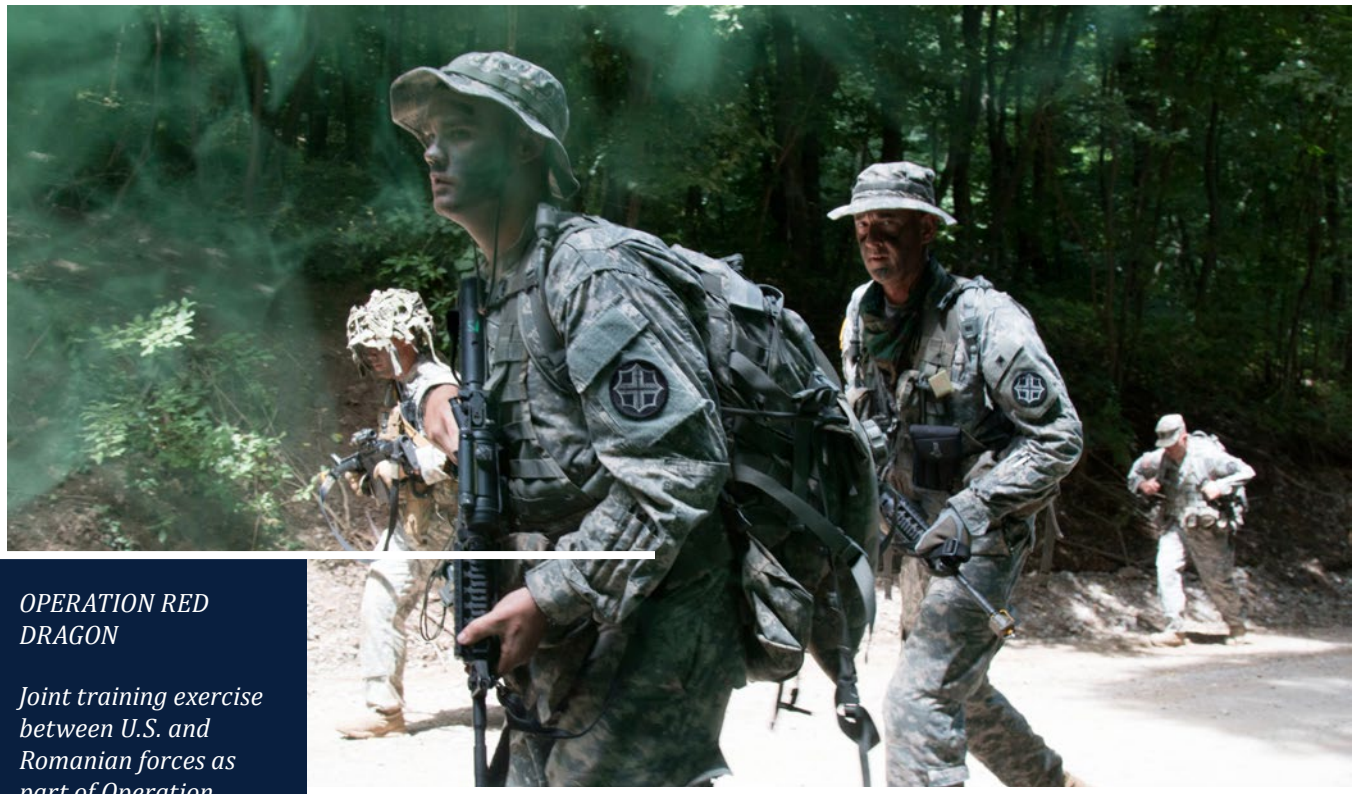
Russia is making a significant investment in building its military capabilities. It has modernized its forces to develop, for example, an asymmetric, unconventional warfare capability and new weapons systems. It has also enhanced training of its military personnel and units and strengthened their discipline.

Russia's advanced military systems also seek to threaten U.S. advantages in certain areas we have traditionally dominated, such as the capability to disrupt battlefield communications and the use of precision artillery. This has prompted the United States and NATO allies to reinforce their internal security capacity to deter or respond to Russian aggression. In addition, the United States and NATO are committed to building the military capabilities of the Baltic Republics, as well as those of Poland and Romania, through training, advising, and equipping their forces.

Russia's advanced military systems also seek to threaten U.S. advantages in certain areas we have traditionally dominated, such as the capability to disrupt battlefield communications and the use of precision artillery.

According to White House officials, through the European Reassurance Initiative, the DoD is seeking to build the resilience and capability of our allies and partners and to enable a quicker and more robust response in support of NATO's common defense. This initiative increases the presence of U.S. and NATO forces in Europe through stepped-up unit rotations and continued deferral of some planned force reductions. In addition, U.S. and NATO forces have deployed units to Baltic countries and Romania, Poland, and Bulgaria. U.S. and NATO forces are also conducting training and joint exercises with these partner countries' security forces. The total U.S. investment in the European Reassurance Initiative has quadrupled over the past year, from $789 million to $3.4 billion proposed for FY 2017.

Iran also poses increased global security threats. Its continued sponsorship of regional terrorist groups and its nuclear ambitions require the DoD to maintain an adequate deterrent capability and ensure



OPERATION RED DRAGON

Joint training exercise between U.S. and Romanian forces as part of Operation Atlantic Resolve.

Photo courtesy of U.S. Army, Staff Sgt. Christopher Shanley

that the United States can immediately respond if Iran commits acts of aggression. For example, as the Secretary of Defense stated in in his testimony on March 17, 2016, "We must still deter Iranian aggression and counter Iran's malign influence against our friends and allies in the region, especially Israel, to whom we maintain an unwavering and unbreakable commitment." According to the 2017 DoD Defense Posture Statement, Iran supports the Assad regime in Syria, backs Hezbollah in Syria and Lebanon, and is contributing to disorder in Yemen, while still directing hostility and violence to the United States' closest ally in the region, Israel.

Finally, the threat from terrorism and the other strategic threats discussed above underscore the DoD's need to maintain an adequate deterrent capability. Given the simultaneous nature of the evolving threats, the need for continual upgrades in weapons systems and force readiness is a challenge particularly under the resource constraints imposed by the DoD budget. These and other related management challenges are discussed throughout this document. We address in the next section of this document the need for interagency cooperation in addressing these five evolving global threats.

ARTILLERY SUPPORT

Artillery units in Iraq serve two roles: to provide force protection for Coalition and Iraqi security forces and to support ISF ground maneuver, enabling them to defeat ISIL.

Photo courtesy of U.S. Army, 1st Lt. Daniel I Johnson/Released

Interagency Cooperation

The DoD must work with other key elements of the U.S. Government to confront evolving strategic challenges. Interagency cooperation and unity of effort are fundamental to countering global threats successfully. For example, in September 2014, President Obama announced a comprehensive strategy to degrade and ultimately destroy the Islamic State in Iraq and the Levant (ISIL), setting out nine strategic lines of effort to combat its terrorist activities. These nine lines of effort cross agency lines and include active military operations throughout the world, financial and investigative activities among coalition partners, cutting off terrorists' resources, countering ISIL's messaging, and law enforcement activities that protect the homeland. Each line of effort is assigned a designated lead agency or agencies for coordinating and implementing activities, including the Departments of Defense, State, Treasury, and Homeland Security, as well as the U.S. Agency for International Development, the Director of National Intelligence, and the National Counterterrorism Task Force.

Interagency cooperation in the oversight of these activities is critical. For example, section 8L of the Inspector General Act of 1978, as amended, mandates that a Lead Inspector General (IG) develop and carry out a joint strategic plan to conduct comprehensive oversight of all aspects of

contingency operations. The DoD IG has been appointed the Lead IG for the two current contingency operations for Operation Inherent Resolve (OIR), the effort to degrade and destroy ISIL, and Operation Freedom's Sentinel (OFS), the effort to provide support to Afghanistan to help build and sustain an enduring security capability. The Inspectors General for the U.S. Department of State and U.S. Agency for International Development are key partners in fulfilling the oversight requirements associated with the Lead IG activities. The objective of Lead IG oversight is to ensure adequate oversight of any contingency operation through either joint or individual audits, inspections, and investigations. The Lead IG and supporting IGs continue to identify and make recommendations to correct inefficiencies and ineffectiveness in programs throughout their respective agencies. These cooperative efforts are ongoing and collectively reported on a quarterly basis.

In short, the DoD, individually and through interagency efforts, faces a difficult management challenge to effectively combat evolving and growing strategic threats throughout the world.

COUNTER-TERRORISM TACTICS
Partnership for Peace, NATO, and Nordic nations participate in counter-terrorism tactics exercise to prepare for international deployments and defense against terrorism.
Photo courtesy of U.S. Air Force, Staff Sgt. Jonathan Snyder

the Challenge—#2

Countering the Terrorist Threat

As noted in the previous section, countering terrorist threats remains a top challenge and a critical national security priority. For example, on September 27, 2016, the Director of the National Counterterrorism Center testified before Congress stating, "Having passed the 15-year mark since 9/11, the array of terrorist actors around the globe is broader, wider, and deeper than it has been at any time since that day." He added, "The threat landscape is less predictable and, while the scale of the capabilities currently demonstrated by most of these violent extremist actors does not rise to the level that core al-Qaida had on 9/11, it is fair to say that we face more threats originating in more places and involving more individuals than we have at any time in the past 15 years."

GLOBAL COALITION TO COUNTER ISIL

Discussion of priorities for the Coalition's multiple lines of effort.

Photo courtesy of U.S. Air Force Tech. Sgt. Brigitte N. Brantley/Released

In its strategic guidance document, "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense," the DoD identified countering "non-state threats" as part of a complex set of challenges in the global security environment. The document further stated that the DoD will continue working with allies and partners to establish control over ungoverned territories and directly strike the most dangerous groups and individuals when necessary.

With regard to threat to DoD forces and insider threats, in a recent statement to the Senate Armed Services Committee, Secretary Carter discussed the importance of countering the terrorist threat to DoD personnel and facilities. He stated that the DoD is working to ensure "force protection for our troops and the DoD facilities where they work and reside—both on base, and the thousands of off-base installations we operate. Last summer's tragedy in Chattanooga Tennessee, underscored how ISIL seeks to target U.S. troops and DoD civilians, which is why we're putting in place stronger physical security systems, including stronger entry controls, better alarm systems, reinforced doors, additional ways to safely exit our facilities, and more."

In addition to threats posed by foreign entities, the DoD also seeks to counter internal threats by developing insider threat programs to deter, detect, and mitigate actions by employees who may represent a threat

to national security. According to the National Counterintelligence and Security Center, "the most damaging U.S. counterintelligence failures, over the past century, were perpetrated by a trusted insider with ulterior motives."

DoD views building partnership capacity as an essential strategy in helping to respond to terrorism as well as sharing the costs and responsibilities of this ongoing challenge.

Building Partner Capacity

According to its strategic guidance document, the DoD views building partnership capacity as an essential strategy in helping to respond to terrorism as well as sharing the costs and responsibilities of this ongoing challenge. Accordingly, the DoD's strategy addressed regional military challenges by partnering with and helping to develop the military capabilities of allied nations. A major DoD program for working with foreign militaries is the Defense Institution Building program, which is managed by the Defense Security Cooperation Agency. The Defense Institution Building Program's aim is to establish responsible defense governance to help partner nations build effective, transparent, and accountable defense institutions.

In Iraq, the United States and its coalition partners are engaged in OIR, the mission to degrade and destroy ISIL. According to the 2017 Defense Posture Statement, the U.S. strategy includes providing military support to coalition partners and making significant investments in training, advising, assisting, and equipping the Iraqi Security Forces (including Kurdish and Sunni Popular Mobilization forces), and in enabling moderate Syrian anti-ISIL forces.

This is a difficult mission with no easy solutions, particularly in Syria. The train, advise, assist, and equip program is essential to building the capacity of Iraqi security forces. Iraqi Sunni tribal forces and vetted Syrian opposition forces were key to OIR progress in 2016. Iraqi Sunni tribal forces supported the liberation of Sunni-dominated Falluja, and the Syrian fighters succeeded in liberating Manbij and closing the Turkish border to ISIL.

Several DoD OIG oversight reviews examined aspects of the fight against ISIL. For example, a September 2015 DoD OIG assessment evaluated U.S and Coalition efforts to train, advise, and assist the Iraqi Army to initiate and sustain combat operations to defeat ISIL. The report made recommendations that the U.S and Coalition authorities update operational and program plans, communications and quality assurance processes, and improve the mentorship of Ministry of Defense personnel.

Ongoing DoD OIG oversight efforts are assessing U.S and Coalition efforts to train, advise, assist, and equip the Kurdish Security Forces, the Iraqi Counterterrorism Service, and Iraqi Special Operations Forces. Future oversight will examine U.S and Coalition efforts to build the capacity of the Iraq Federal Police, DoD's analysis of information contained in social media in support of OIR, and whether DoD and the U.S. Department of State are effectively planning and coordinating stabilization efforts in Iraq and Syria.

In Afghanistan, the United States is conducting operations through OFS against terrorist groups in the region. The United States is also supporting the NATO-led Resolute Support Mission to develop the institutional capacity of Afghanistan's Ministries of Defense and Interior to support and sustain the Afghan National Defense and Security Forces (ANDSF). The United States faces ongoing challenges in its efforts to develop a self-sustaining ANDSF. Moreover, the pace of progress in building Afghan national institutions and effective leadership within those institutions is slow and may be insufficient to achieve broad U.S. objectives in a reasonable time frame.

The pace of progress in building Afghan national institutions and effective leadership within those institutions is slow and may be insufficient to achieve broad U.S. objectives in a reasonable time frame.

Prior DoD OIG oversight in Afghanistan identified key challenges in these efforts, such as inadequate capacity of the Ministries of Defense and Interior to lead and sustain the ANDSF; poor asset accountability and sustainment of vehicles and equipment; and insufficient logistic sustainment capability within the Afghan National Police. Shortcomings in building adequate systems to sustain growing Afghan security forces is a recurrent theme in DoD OIG oversight work and underlies many of the ANDSF capability gaps that have been identified. For example, the DoD OIG has found that mechanisms to provide supplies, equipment, maintenance, and personnel to Afghan army and police forces remain immature and unreliable.

Other oversight organizations, such as the Special Inspector General for Afghanistan Reconstruction (SIGAR) have identified challenges with building partner capacity. For example, an April 2016 report, coauthored by SIGAR and the U.S. Institute of Peace, identified lessons learned in the international efforts to rebuild Afghanistan. The report cited a number of challenges, including the need to address conflicting goals held by the various parties involved in Afghanistan. The report noted that warfighting goals are focused on immediate effects on the battlefield while developmental goals focused on sustainable achievements resulting from multiyear efforts. The report found that many nations were unclear as to what they were trying to achieve in Afghanistan or how to prioritize their warfighting versus development goals.

The report also found that the Coalition lacked shared, well-defined donor objectives and goals. Finally, with regard to improving chances for success in Afghanistan, the report noted that the success of development efforts hinged on donors' knowledge of the local areas and their ability to gain the buy-in of Afghans living there. However, donors' ability to tailor their efforts to local needs was often undermined by inappropriate measures of progress, inability to move around the country, and frequent rotation of personnel.

Future DoD OIG oversight will examine the Afghan Ministry of Interior's development of its internal controls capability; the Afghan government's controls over U.S. direct funding assistance; and U.S and Coalition efforts to train, advise, and assist the Afghan Air Force. DoD OIG intelligence assessments will also focus on U.S. counterterrorism capabilities and effectiveness in support of OIR and OFS.

In an April 2016 review, the Government Accountability Office (GAO) cited building partner capacity as a central focus of the U.S. counterterrorism strategy, as underscored by the allocation of $675 million for Global Train and Equip program activities in fiscal year 2015. The allocation was a sharp increase compared to the $275 million annual average in the preceding 6 years. The GAO concluded that although DoD had established an interagency process to develop and select security assistance project proposals, the DoD did not require documentation of receiving units' capacity to absorb the assistance offered or fully document consideration of other key elements in planning fiscal year 2015 projects. According to the GAO, fully documenting the basis of project approval decisions could enhance transparency, provide additional assurance that resources are efficiently allocated, and help ensure the long-term benefits of projects and careful use of scarce U.S. and partner nation resources.

Insider Threat

It is also important to recognize that threats to the United States, its citizens, and its military can come from insider threats, not only foreign governments and terrorist groups. Perhaps the most compelling recent example of an insider threat that has caused great harm to U.S. intelligence gathering capabilities is the case of Edward Snowden. He is the former National Security Agency contractor employee who remains a fugitive due to his admitted theft and release of classified National Security Agency information. In 2014, President Obama stated that Snowden's leaks of

classified information revealed "methods to our adversaries that could impact our operations in ways that we may not fully understand for years to come."

Insiders can further commit terrorist acts or cause harm to U.S. personnel or organizations because they have an awareness of their organization's vulnerabilities or exploitable security measures. Insiders can engage in terrorist activities through compromising sensitive information or through the use or threat of violence.

Insiders can commit terrorist acts or cause harm to U.S. personnel or organizations because they have an awareness of their organization's vulnerabilities or exploitable security measures.

For example, in November 2009, an Army officer shot and killed 13 people and wounded 32 others on base at Fort Hood, Texas. That officer had exchanged e-mails with an al Qaeda figure asking whether individuals that attack fellow soldiers were considered martyrs. In September 2013, a Navy contractor killed 12 civilian employees and contractors and wounded 4 others at the Washington Navy Yard, D.C., in an act of workplace violence.

DoD's reviews of each incident resulted in numerous recommendations associated with personnel policy, installation security, force protection, casualty response, and support to DoD healthcare providers. A July 2015 GAO report concluded that the majority of policy and guidance related to DoD's key force protection had been updated, but some guidance did not yet reflect insider threat considerations. The GAO further found that while selected installations have taken actions to protect against insider threats, the DoD has not consistently shared this information, and the DoD was still in the process of implementing recommendations from the Fort Hood and Washington Navy Yard reviews.

In May 2016, the DoD required contractors, for the first time, to establish and implement their own insider threat program to detect, deter, and mitigate insider threats. The revised National Industrial Security Program Operating Manual requires contractors to have a written program plan in place to begin implementing revised insider threat requirements no later than November 30, 2016.

In 2014, the DoD also created the Insider Threat Management and Analysis Center and DoD Component Insider Threat Records System. The system's purpose is to analyze, monitor, and audit insider threat information for insider threat detection and mitigation within DoD concerning DoD and U.S. Government installations, facilities, personnel, missions, or resources. The system supports insider threat programs, enables the identification of systemic insider threat issues and challenges, provides a basis for the

FORT HOOD, TX

Soldiers praying at the Memorial Service held for those killed in the Fort Hood shooting.

Photo courtesy of U.S. Army, Sgt. Ken Scar, 7th Mobile Public Affairs Detachment

development and recommendation of solutions to mitigate potential insider threats, and assists in identifying best practices amongst other Federal Government insider threat programs. Future DoD OIG oversight will assess whether the DoD Insider Threat Management and Analysis Center has adequate controls over the collection, analysis, and dissemination of insider threat and workplace violence information.

To address insider threat concerns involving the security of military housing, the DoD OIG reviewed access controls for general public tenants leasing housing on military installations and found that DoD officials did not ensure that tenants were properly screened before granting unescorted access to installations. Additionally, access badges were issued with expiration dates that exceeded tenants' lease terms. As a result, the DoD assumed an unnecessary safety and security risk to military personnel, their dependents, civilians, and assets.

In sum, while the DoD recognizes the challenges posed by insider threats, they remain a vulnerability and require continued focus from the DoD.

ACQUISITION CHALLENGES
The guided-missile destroyer Pre-Commissioning Unit Zumwalt is the first in a three-ship class of the Navy's newest, most technologically advanced multi-mission guided-missile destroyers.

Photo courtesy of U.S. Navy, Haley Nace/ Released)

the Challenge—#3

Enabling Effective Acquisition and Contract Management

Acquisition and contract management have been high-risk areas for the DoD for many years. Although Congress and the DoD have long sought to improve the acquisition of major weapon systems, many DoD programs are still falling short of cost, schedule, and performance expectations. This can result in unanticipated cost overruns, program development spanning decades, and, in some cases, a reduction in the capability ultimately delivered to the warfighter.

In addition to acquisition challenges, the DoD obligates more than $300 billion annually on contracts for goods and services, including support for military installations, information technology, consulting services, and commercial items. The DoD must also reengineer its processes to evaluate contracts for spare parts pricing and manage its contracts for weapons system support.

Furthermore, the DoD must continually focus on preventing the illegal transfer of operational and defense technologies.

Acquisition Challenges

The scope and size of acquisition programs for DoD weapon systems is enormous. As of April 2016, the DoD portfolio of defense acquisition programs totaled 1,375 programs. In the FY 2017 Presidential Budget, the DoD requested $183.9 billion to fund those acquisition programs. Over the past year, the number of programs in the DoD portfolio of major defense acquisitions increased from 78 to 79, while its total planned investment in these programs decreased from $1.45 trillion to $1.44 trillion.

In recent years, the DoD has taken steps to improve the acquisition of major weapon systems, such as implementation of DoD's Better Buying Power initiatives. In 2010, the DoD launched these initiatives to strengthen the DoD's buying power; improve industry productivity; and provide an affordable, value-added military capability to the warfighter. The Better Buying Power initiatives provide a set of fundamental acquisition principles to achieve greater efficiencies through affordability, cost control, elimination of unproductive processes and bureaucracy, and promotion of competition. The initiatives are also designed to incentivize productivity and innovation in industry and Government, and improve the processes for the acquisition of services.

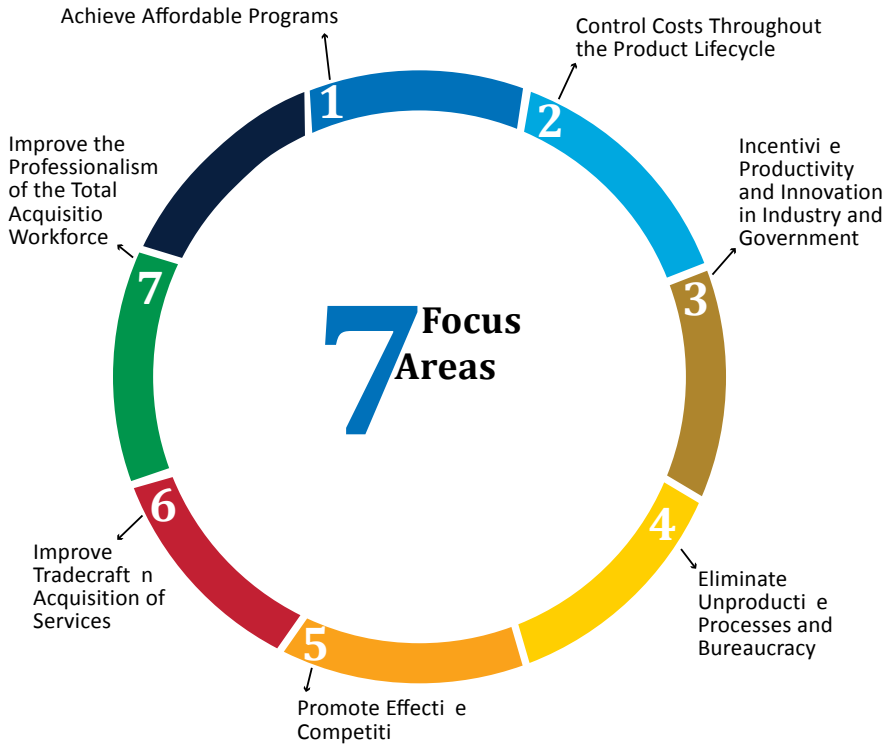
Acquisition programs continue to exceed the cost and schedule defined in the program's strategy documents.

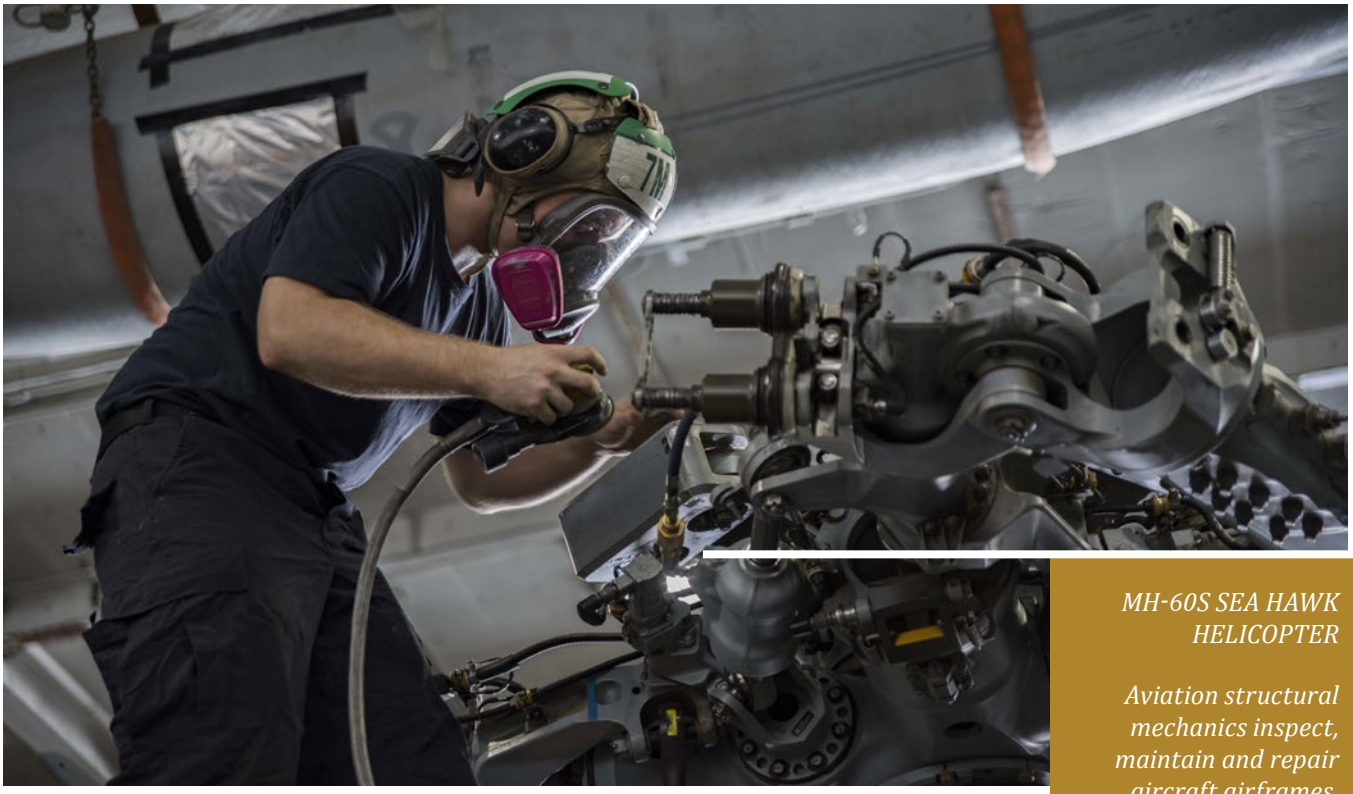
Despite this initiative and these positive steps, acquisition programs continue to exceed the cost and schedule defined in the program's strategy documents. DoD OIG audits have found program managers contribute to acquisition challenges by approving concurrent development and testing of software and hardware during production that expose programs to undue risks of additional design changes and costly retrofits. For example, the DoD OIG evaluated the Navy's efforts to prepare and manage the Ship-to-Shore Connector ship acquisition program for initial production. The DoD OIG found that program officials' plan to conduct concurrent developmental testing and production may require the Navy to make substantial and costly modifications resulting from design and integration deficiencies found during production. The DoD OIG found in other audits that some programs are proceeding into production before manufacturing processes are fully established, which causes cost and schedule delays.

According to the DoD, the promotion of competition is a central tenet in acquisition reform and the single best way to motivate contractors to provide the best value. However, a GAO assessment of weapons programs found inconsistent use of acquisition strategies that include competition. Of 43 programs that GAO assessed as a part of its 2016 selected weapon programs assessment, 21 programs conducted or planned to conduct competitive prototyping before development start and 26 had acquisition strategies that included some measure to encourage competition after development start. In addition, 13 programs reported pursuing measures to promote competition both before and after the start of system development. GAO found that those programs experienced less development cost growth than those that promoted competition in only one phase of acquisition. GAO also reported its prior work has shown that competitive prototyping can help programs reduce technical risk, refine requirements, and validate designs and cost estimates prior to making major commitments of resources. Programs that do not take this step may miss an opportunity to lower costs and reduce risk.

Better Buying Power

Better Buying Power (BBP) is the implementation of Best Practices to strengthen the Defense Department's buying power, improve industry productivity, and provide an affordable, value-added military capability to the Warfighter





MH-60S SEA HAWK HELICOPTER

Aviation structural mechanics inspect, maintain and repair aircraft airframes.

Photo courtesy of U.S. Navy, Seaman Christopher A. Michaels

Overall, DoD OIG audits have determined that the DoD has made progress in acquisition program management, but the DoD continues to experience programmatic problems, such as cost overruns and schedule delays in acquisition programs. For example, the DoD OIG has continued to identify acquisition challenges in which:

- program personnel inappropriately requested waivers and deferrals from operational test requirements;
- program personnel certified that programs were ready for initial operational test and evaluation when programs were not;
- program personnel did not adequately document the acquisition process to define, validate, fund, and execute requirements; and
- programs did not meet system performance requirements.

Additionally, the DoD OIG continues to identify other challenges in the acquisition process. For example, contracting personnel did not:

- always determine fair and reasonable prices for spare parts,
- acquire excess spare parts inventory, and
- adequately manage contracts for weapons system support.

DoD OIG determined that the Army should specifically define the capability requirements to increase the likelihood that the Integrated Air and Missile Defense Battle Command System would provide useful and supportable capabilities that could be effectively developed, tested, and produced at an affordable cost.

The DoD OIG made specific recommendations to address these challenges, and the Services have made progress in implementing them. For example, the DoD OIG evaluated the Navy's management of waivers and deferrals from operational test requirements for nine major weapon systems. The DoD OIG review of waiver requests at the Naval Air Systems Command found that Navy program managers and system sponsors did not fully implement Navy policies for requesting waivers and deferrals before certifying if the programs were ready for Initial Operational Test and Evaluation to support the final production decision. As a result, six of nine programs reviewed completed Initial Operational Test and Evaluation with unresolved deficiencies that negatively impacted the warfighter's primary missions. The Navy took immediate actions by issuing interim guidance to address the gaps in the testing and identification of deficiencies caused by program offices unchecked use of the waiver and deferral process. Additionally, the Vice Chairman of the Joint Chiefs of Staff updated the Manual for the Operation of the Joint Capabilities Integration and Development System to include a requirement that program managers notify Joint Requirement Oversight Council when a program is not meeting its primary mission requirement. In another review, the DoD OIG found that the Army plans to spend $2.52 billion over 20 years to procure and maintain 501,289 carbine rifles that its own analysis shows could be delayed for another 10 years with no negative impact to the warfighter. The Army agreed with the DoD OIG recommendation to eliminate funding for the program.

In another example, the DoD OIG determined that the Army should specifically define the capability requirements to increase the likelihood that the Integrated Air and Missile Defense Battle Command System, valued at approximately $6.4 billion, would provide useful and supportable capabilities that could be effectively developed, tested, and produced at an affordable cost. The Under Secretary of Defense for Acquisition, Technology, and Logistics agreed to postpone the initial production decision until the project manager completes testing that shows the Army system will meet the planned requirements. The Commander, Army Fires Center of Excellence, agreed to fully define system capability requirements for the planned second increment of the system.

Moreover, the acquisition of weapon systems that meet warfighter requirements is critical to enabling the United States to implement its strategic military plans. From 2001 through 2014, test results for 123 weapons systems developed as major defense acquisition programs showed that over 40 percent of weapons systems managed as major

NAVY NEXT GEN

F-35 Stealth Strike Fighter Flies Over Next Gen Stealth Guided-Missile Destroyer, USS Zumwalt

Photo courtesy of U.S.Navy, Andy Wolfe/Released

defense acquisition programs could not fully meet mission requirements at the time of initial deployment. The discovery of programs not meeting performance requirements at this late phase of the development process results in further unforeseen delays.

Software development is one major factor that affects the ability of weapon systems to meet mission requirements. In a March 2016 assessment of selected DoD weapons programs, the GAO found that of 55 programs assessed, 40 reported software development as a high-risk area. According to the GAO report, the three most common reasons for high risk in software development were the challenge of completing the software development needed to conduct developmental testing; underestimating the difficulty of the originally planned software effort; and hardware design changes that necessitate additional software development.

Despite DoD's efforts to reduce waste, accelerate schedules, and control costs, new weapon systems are regularly fielded later than originally planned, which results in increased expenses in DoD's acquisition programs. Part of the problem is that weapons manufacturers are incentivized to submit optimistic cost and schedule estimates to be awarded major contracts. Service officials may agree with these projections to protect their acquisition budgets. Weapons system program

managers, caught in the middle, want to avoid disruption stemming from comparing optimistic cost estimates with unrealistic performance requirements after their programs have started.

Since FY 2013, the DoD OIG has identified about $31 billion in acquisition program quantities that were not validated or properly approved.

The DoD OIG typically audits programs that are 15 to 18 months from a major acquisition milestone decision. Since FY 2013, the DoD OIG has identified about $31 billion in acquisition program quantities that were not validated or properly approved. Additionally, the DoD OIG have determined the capability requirements have not been adequately defined and tested and that test community recommendations or deficiencies have not been adequately addressed and, in some cases, ignored. Acquisition reform has not alleviated DoD OIG findings that programs continue to exceed cost and schedule baselines and have not adequately defined performance metrics.

In FY 2017, the DoD OIG plans to perform additional audits on the acquisition process, including acquisitions on programs such as the Navy Expeditionary Fast Transport program, Marine Corps Amphibious Assault Vehicle, Navy Mine Countermeasures Mission Package, and Army and Marine Corps Joint Light Tactical Vehicle.

Contract Management and Oversight

The DoD spends approximately $300 billion each year on contracts for services and supplies. It faces challenges with contracting for sustainment contracts, procuring domestically produced items, contracting with small business, oversight of contracting officer's representatives (CORs), and completing assessment reports on contractor performance.

DoD OIG oversight of DoD's contracting continues to identify challenges with sustainment contract costs. For example, the DoD OIG identified an Air Force contract in which, over a 4-year period, $1 billion was spent without achieving its acquisition objective of increasing aircraft availability while decreasing sustainment costs. Also, in another instance, the DoD OIG found that DoD invested in a modernization program to update its aircraft, reduce operating costs, and extend the service life for decades without fully validating almost $60 million in sustainment costs.

The DoD also struggles to comply with the Berry Amendment and the Buy American Act. The Berry Amendment promotes the purchase of goods produced in the United States by directing how the DoD can use funds to purchase items such as fabrics, food, and hand tools. The Buy American Act of 1933 requires, with certain exceptions, that only articles, materials, and supplies that have been mined, produced, or manufactured in the

United States are used to fulfill Federal procurement and construction contracts. Overall, the DoD OIG has found that the Services did not consistently comply with the Berry Amendment and the Buy American Act. Contracting personnel were not always familiar with legal and DoD requirements to procure items produced in the United States. Additionally, contracting personnel issued contracts that did not include the appropriate contract clauses to implement the Berry Amendment and Buy American Act. Service personnel had limited assurance that the purchased items complied with the Buy American Act, and suppliers may have provided items that were not produced in the United States. Contracting personnel also may have violated the Antideficiency Act when they used appropriated funds to purchase non-domestically produced items when domestically produced items were available.

The Federal Acquisition Regulation requires the Federal Government to provide maximum practicable opportunities in its acquisitions to small business. Small businesses must also have the maximum practicable opportunity to participate as subcontractors in the contracts awarded by any executive agency that is consistent with efficient contract performance. The DoD's contracting with small businesses has improved. For example, in FY 2015, the DoD exceeded its goal for awarding prime contracts to small businesses.

The DoD OIG's work has identified that the DoD is at risk for contractors passing inflated costs to the DoD but not savings. Furthermore, subcontract evaluations present additional challenges. Major subcontractors often represent 50 percent or more of total cost on major defense acquisition programs. Prime contractor access to subcontractor cost or pricing data, including historical actual costs, may be limited, resulting in the DoD overpaying for those subcontractor costs. As of August 2016, the DoD OIG identified that the DoD spent at least $194 million more than fair and reasonable prices for commercial and noncommercial spare parts. Additionally, we estimate that the DoD could spend an additional $402.5 million more than fair and reasonable prices for spare parts based on expected future use. This is a systemic challenge that has not vastly improved, although the DoD OIG has issued more than 30 reports on spare-part pricing in the last 18 years.

As of August 2016, the DoD OIG identified that the DoD spent at least $194 million more than fair and reasonable prices for commercial and noncommercial spare parts.

The DoD also continues to struggle with providing effective contract oversight. Specifically, DoD OIG audits determined that contracting officers did not always appoint CORs, CORs were not always adequately trained, contracting officials did not always develop adequate quality assurance surveillance plans or were missing them altogether, and CORs

COMBINED WEAPONS TRAINING

Marines head out to simulate a battalion coil on a Light Armored Vehicle 25.

Photo courtesy of U.S. Marine Corps, Cpl. Melodie Snarr/ Released

did not always maintain supporting documentation. Some contracting officers did not define responsibilities for CORs, or assigned multiple contracts to one COR who may not have had sufficient time to perform all oversight responsibilities. The CORs did not use the oversight procedures established in the quality assurance surveillance plan to monitor contractor performance.

Without effective oversight by CORs, the DoD will not have sufficient information to assure goods and services received are consistent with contract quality requirements and performed in a timely manner.

The DoD OIG has also identified significant problems with past performance reporting across the DoD. The Federal Acquisition Regulations require that contractor performance information be collected and used in source selection evaluations. Source selection officials should rely on clear and timely evaluations of contractor performance to make informed business decisions when awarding Government contracts and orders. This information is critical to ensuring that the Federal Government only does business with companies that provide quality products and services in support of DoD missions. DoD OIG audits have found that DoD officials have not evaluated contractor performance in accordance with guidance.

Illegal Technology Transfer

Technological superiority is critical to U.S. military strategy. The DoD spends billions each year to develop and acquire sophisticated technologies that provide an advantage for the warfighter during combat or other missions. Many of these technologies are also sold or transferred to other countries to promote U.S. economic, foreign policy, and national security interests. These technologies can also be acquired through foreign investment in U.S. companies that develop or manufacture them. However, sensitive DoD technology is also a target for unauthorized transfer, such as theft, espionage, reverse engineering, and illegal export.

The DoD spends billions each year to develop and acquire sophisticated technologies that provide an advantage for the warfighter during combat or other missions.

The DoD continues to face the challenge of preventing the illegal transfer of these sensitive technologies. To avoid illegal technology transfer, U.S. technology must be transferred in accordance with U.S. export control laws. The U.S. Export Control Act regulates the transfer of U.S. technology, including arms and defense technology.

Each year, the Defense Security Service publishes a report of its findings on foreign attempts to collect sensitive or classified information and technology. In the FY 2015 report, the Defense Security Service reported a continued increase in reported foreign collection attempts to obtain sensitive or classified information and technology. These collection attempts targeted all aspects of DoD technologies, including electronics; command, control, communication, and computers; aeronautic systems; and marine systems.

The Defense Security Service report identified the most common methods of operation, including academic solicitation, suspicious network activity, and attempted acquisition of technology through commercial, government, and government-affiliated organizations. The report stated that the threat faced by illegal transfer of DoD technology "shows no sign of waning, and securing our cutting-edge technology remains key to maintaining our military and economic advantage."

The DoD has published agency-wide policies and worked to strengthen programs to identify and protect technologies critical to U.S. interests. The Defense Security Service administers the National Industrial Security Program for DoD and 30 other Federal agencies. Recognizing that U.S. industries develop and produce the majority of U.S. defense technology, the National Industrial Security Program ensures DoD contractors properly safeguard classified information and information associated with critical technologies. To remain a facility that is cleared by the National Industrial Security Program, DoD contractors must meet specific requirements to

ensure they are safeguarding critical technologies in their possession while negotiating bids, contracts, programs or performing research and development efforts. DoD policy requires DoD organizations and contractors to report unlawful attempts to access or illegally transfer critical technologies to the appropriate counterintelligence or law enforcement agency.

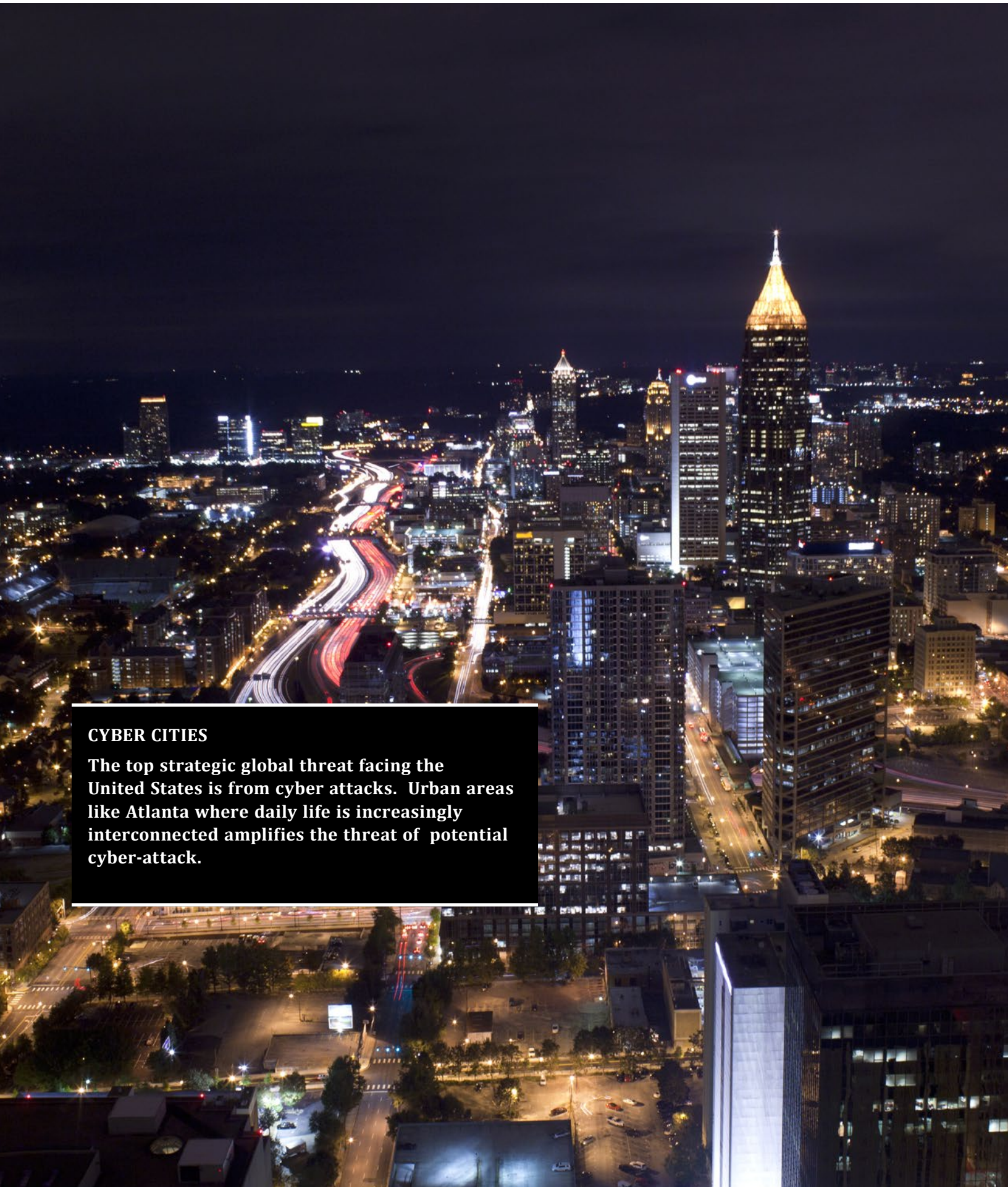
As the criminal investigative arm of the DoD OIG, the Defense Criminal Investigative Service (DCIS) conducts counter-proliferation investigations that pertain to the illegal transfer of sensitive DoD technologies.

As the criminal investigative arm of the DoD OIG, the Defense Criminal Investigative Service (DCIS) conducts counter-proliferation investigations that pertain to the illegal transfer of sensitive DoD technologies. As of September 30, 2016, the DCIS had 198 open counter-proliferation cases that represent approximately 12 percent of its active investigations. In FY 2016, the DCIS counter-proliferation investigations resulted in 12 criminal charges, 11 convictions, and over $20 million in recoveries for the Government.

The DCIS routinely works with counterpart Federal law enforcement agencies and de-conflict investigative activity through the Department of Homeland Security's Export Enforcement Coordination Center. The following examples highlight a few of recent DCIS investigations.

Three Chinese Nationals affiliated with the Chinese company HK Potential were arrested in Connecticut and convicted for a scheme to steal and illegally export sophisticated U.S. military semiconductors. These semiconductors were designed for ballistic missile and satellite applications. To conceal the theft, the perpetrators provided counterfeit semiconductors to replace the original semiconductors. One defendant has been sentenced to 15 months confinement and was ordered to forfeit $63,000. The other two defendants are awaiting sentencing. In a separate case, a California woman was convicted and sentenced to 50 months in prison for conspiring to export fighter jet engines, an unmanned aerial vehicle and related technical data to China in violation of the Arms Export Control Act. In another example, a Chinese National was arrested for illegally attempting to export high-grade carbon fiber to China. The individual allegedly expressed a willingness to pay a premium to avoid U.S. export laws. The carbon fiber, which has many aerospace and defense applications, is strictly controlled.

In short, the DoD has initiated several initiatives to improve its acquisition and contract management processes. However, more needs to be done to reduce the high risks within acquisition and contract management. In addition, steps need to be taken to ensure arms and defense technology must be transferred in accordance with U.S. export control laws.



CYBER CITIES

The top strategic global threat facing the United States is from cyber attacks. Urban areas like Atlanta where daily life is increasingly interconnected amplifies the threat of potential cyber-attack.

the Challenge—#4

Increasing Cyber Security and Cyber Capabilities

Since 2013, the Director of National Intelligence has identified cyber threats as the top strategic global threat facing the United States. In testimony to Congress in 2013 and 2014, the Director cited a wide range of potential adversaries who attempt to disrupt or manipulate U.S. activities, relying on digital technology or the Internet. The GAO also identifies cybersecurity of Federal information systems and networks as a high-risk area because all sectors of the Government—energy, transportation systems, communications, financial services, and defense of the homeland—are dependent on information systems and electronic data to perform operations and to process, maintain, and report essential information.

The DoD has become increasingly reliant on cyberspace to enable its military, intelligence, and business operations to perform the full spectrum of military operations without disruption, and cyber threats and exploitable vulnerabilities have grown substantially. The Secretary of Defense recognized the need to increase the DoD's cybersecurity efforts and has requested $6.7 billion in FY 2017 to support the DoD's cybersecurity efforts,

DoD has become increasingly reliant on cyberspace to enable its military, intelligence, and business operations to perform the full spectrum of military operations without disruption, and cyber threats and exploitable vulnerabilities have grown substantially.

To guide DoD's cyber activities and operations, in 2011 the Secretary of Defense signed the initial "DoD Strategy for Operating in Cyberspace." This document also established the Cyber Mission Force, and, in 2012, the DoD began to build the Cyber Mission Force of approximately 6,200 military, civilian, and contractor support personnel to perform critical DoD cyber missions. The Cyber Mission Force performs defensive cyberspace operations, defends the United States and its interests against cyberattacks, and supports combatant commands in integrating cyberspace effects into command plans.

In April 2015, the Secretary of Defense issued a new DoD Cyber Strategy to build upon the initial concepts and set prioritized goals and objectives through 2020. This strategy defines three separate, but interdependent DoD cyber missions:

- defend DoD Information Networks, systems, and information;
- defend, in coordination with the Department of Homeland Security and other Federal agencies, the U.S. homeland and U.S. national interests against cyberattacks; and
- support combatant command operational and contingency planning.

In addition to the Cyber Mission Force buildup, the DoD has invested about $20 billion since 2012, earmarked for cybersecurity enhancements and technology acquisitions to improve its ability to protect DoD and U.S. interests from cyberattacks.

The Commander, U.S. Cyber Command, who is responsible for leading DoD offensive cyberspace operations, stated that the DoD has made progress in developing strategies and goals to combat cyber threats. However, the DoD continues to face significant challenges in protecting and securing its networks, systems, and infrastructure from cyber threats and in increasing its overall cyber capabilities. Cyberspace threats to the DoD continue to increase at an alarming rate. In April 2016, the Commander reported

that cyberspace operations by a range of state and non-state actors have intensified against the DoD. The Commander cited individual criminal acts as the most significant number of attacks but noted that nation states, such as Russia, China, Iran, and North Korea, still represent the gravest threats to national security because they have the skills, resources, and patience to sustain sophisticated campaigns to penetrate and compromise DoD's networks. The Commander also stated that cyberattacks against the power grid, communications networks, and vital U.S. services could significantly affect command and control of DoD operations and, more broadly, the basic business functions of the United States.

Among other significant cyberattacks, North Korea conducted a cyberattack against Sony Pictures Entertainment, and the Chinese conducted a cyberattack against the Office of Personnel Management. Both cyberattacks affected security and had significant economic impacts. More recently, well-publicized cyberattacks have breached systems used by the Democratic National Committee, the Democratic Congressional Campaign Committee, and the World Anti-Doping Agency.

Defending DoD Information Technology Networks

DoD established the Joint Force Headquarters–DoD Information Network in January 2015 to lead and coordinate command and control decisions and tactical operations affecting the defense of DoD's systems, networks, and data.

The DoD must defend its many information technology networks, both unclassified and classified, from compromise. This is a significant challenge. The DoD Information Network is a globally interconnected, end-to-end set of information capabilities that collects, processes, stores, disseminates, and manages critical information. It includes owned and leased communications and computing systems and services, software, data, and security and other associated services. The network seeks to design, build, configure, secure, operate, maintain, and sustain DoD communications systems and networks in a way that creates and preserves data availability, integrity, and confidentiality, as well as user authentication and nonrepudiation.

To improve its ability to defend the DoD Information Network, the DoD established the Joint Force Headquarters–DoD Information Network in January 2015 to lead and coordinate command and control decisions and tactical operations affecting the defense of DoD's systems, networks, and data. The Commander, Joint Force Headquarters–DoD Information Network, also coordinates with the Commander, U.S. Cyber Command.

The Commander, U.S. Cyber Command, also serves as the Director of the National Security Agency. The Secretary, Congress, and President are considering separating these commands. The GAO is currently assessing, among other things, the advantages and disadvantages of the Commander,

CYBER EXPO

Expo was held to increase awareness of cybersecurity threats and how they impact day-to-day Army operations.

Photo courtesy of U.S. Army, Timothy L. Hale/Released

U.S. Cyber Command, serving as the Director of the National Security Agency and how the DoD measures performance for this relationship in response to a proposed congressional mandate.

To assess the DoD's efforts to protect its information networks, the DoD OIG issued a report in 2013 on maintaining authorization accreditation for select DoD information systems. The report concluded that 2 of the 10 information systems reviewed operated on the DoD Information Network for as long as 14 months without proper security controls to continue their authorization agreements. The DoD OIG recommended that the Air Force take appropriate action to shut down network access or accept the risk of operating without approved security controls for all systems with expired authorities to operate.

The DoD OIG also conducted audits related to the protection of physical and logical access to the Secret Internet Protocol Router Network. The audits found consistent and systemic weaknesses that affected the security of the classified network. The DoD OIG recommended specific physical security improvements and other cybersecurity-related actions to limit access points, account for all circuits, and manage general and privileged account access. Although not completed, the Navy and Air Force have begun corrective actions to address specific and systemic weaknesses identified in these OIG audits.

Developing and Using Cyber Capabilities and Infrastructure

DoD OIG issued a classified report concluding that the Military Services were independently developing cyber platforms and cyber capabilities, which could result in redundant capabilities that do not align with the mission needs of the Cyber Mission Force.

The DoD also faces challenges in developing or acquiring unique cyber capabilities to conduct defensive and offensive operations. In September 2015 testimony, the Deputy Secretary of Defense and the Commander, U.S. Cyber Command, stated that the DoD continues to develop a broad range of cyberspace capabilities and a separate infrastructure to respond to or conduct cyberspace attacks. In November 2015, however, the DoD OIG issued a classified report concluding that the Military Services were independently developing cyber platforms and cyber capabilities, which could result in redundant capabilities that do not align with the mission needs of the Cyber Mission Force. Among other actions, the DoD OIG recommended developing a unified strategic plan to address capability development to meet both Service-specific and joint mission requirements. Although not completed, U.S. Cyber Command and the Military Services have begun to address joint capability development needs of the Cyber Mission Force.

The DoD is now building a unified platform to integrate disparate cyber platforms and capabilities. However, the unified platform will not be operational for several years. To ensure that the Cyber Mission Force and the Services are able to meet joint and Service-specific operational requirements, the DoD needs to unify capability development and accelerate research and development of cyber capabilities, including basic and applied research to develop cyber technologies that can be used in a wide range of operational environments.

Additionally, the DoD is in the process of implementing the Joint Information Environment, an initiative announced in August 2010 by the Secretary of Defense to consolidate information technology infrastructure to achieve savings in acquisition, sustainment, and manpower costs and improve the DoD's ability to defend its networks against growing cyber threats. This is designed, in part, to reduce the DoD Information Network attack surface by establishing a single security architecture, optimizing identity and access management, and migrating to cloud computing. However, since 2014, the DoD OIG and the GAO have issued reports on the DoD's challenges in implementing Joint Information Environment initiatives.

NETWORK MONITORING

I Marine Expeditionary Force Large Scale Exercise included a team of cyber defense specialists with Fleet Cyber Command.

Photo courtesy of U.S. Marine Corp, Cpl. Garrett White

The DoD has been actively engaged with the National Institute of Standards and Technology to improve the understanding of cloud computing across the Federal Government and has implemented enhancements to the DoD's Select and Native Programming Data Input System for Information Technology to more accurately account for cloud budgets and to collect information on DoD cloud contracts.

However, in recent audit reports, the DoD OIG concluded that the DoD did not have an effective cloud computing implementation strategy or process to collect data and measure the effectiveness and efficiency of the DoD cloud initiative. The DoD OIG recommended that the DoD develop an implementation plan that described required tasks, resources, and milestones for transitioning to cloud services and establishing a repository for collecting cloud-related information.

The GAO also issued a report in July 2016 that concluded the DoD's almost $1 billion investment in the Joint Information Environment by yearend FY 2016 has yet to result in fully defining the scope and cost of the program. The GAO recommended defining the scope and expected cost of the Joint Information Environment and fully identifying the composition of the cyber workforce needed to operate within the program. In response to the report, the DoD stated that it was in the process of completing documentation to address new Joint Information Environment program and cost assessments.

Planning and Conducting Defensive and Offensive Operations

Defensive and offensive cyberspace operations, whether conducted individually or simultaneously, are important for defending the U.S. homeland and national interests and supporting operational and contingency operations. In accordance with the October 16, 2012 Presidential Policy Directive-20, "U.S. Cyber Operations Policy," the DoD can conduct offensive and defensive cyberspace operations. For example, as part of OIR, the DoD is conducting offensive cyberspace operations to counter cyber threats and limit disruptive and destructive cyber capabilities used by ISIL and to disrupt and interrupt its ability to operate, communicate, and command and control forces in a digital battlefield. However, the DoD is continuously challenged with attracting and retaining a skilled cyber workforce; limiting vulnerabilities and points of attack to its thousands of systems and networks; developing, testing, and using cyber capabilities; and integrating cyberspace operations into command plans.

DoD is conducting offensive cyberspace operations to counter cyber threats and limit disruptive and destructive cyber capabilities used by ISIL and to disrupt and interrupt its ability to operate, communicate, and command and control forces in a digital battlefield.

The DoD's cyber missions require collaboration with foreign allies and partners. The DoD seeks to build partnership capacity in cybersecurity and cyber defense, and to deepen operational partnerships where appropriate. The DoD is focusing its international engagement on the Middle East, the Asia-Pacific, and key NATO allies.

Building and Retaining DoD's Cyber Workforce

To address the cybersecurity challenge, the DoD must attract and retain a cyber workforce with specialized skills. In 2016, the GAO identified the shortage of cybersecurity professionals in the Federal Government as a high-risk area. Since the DoD began building the Cyber Mission Force in 2012 and fielding teams in FY 2013, it has created 123 of the 133 planned teams with approximately 5,000 of the 6,200 planned personnel. Of these 123 teams, 27 are reportedly fully operational and have supported DoD and other national missions to protect critical systems, networks, and infrastructure. But hiring and retaining these talented and skilled personnel is a difficult challenge for any Government agency, given the intense competition for these skills.

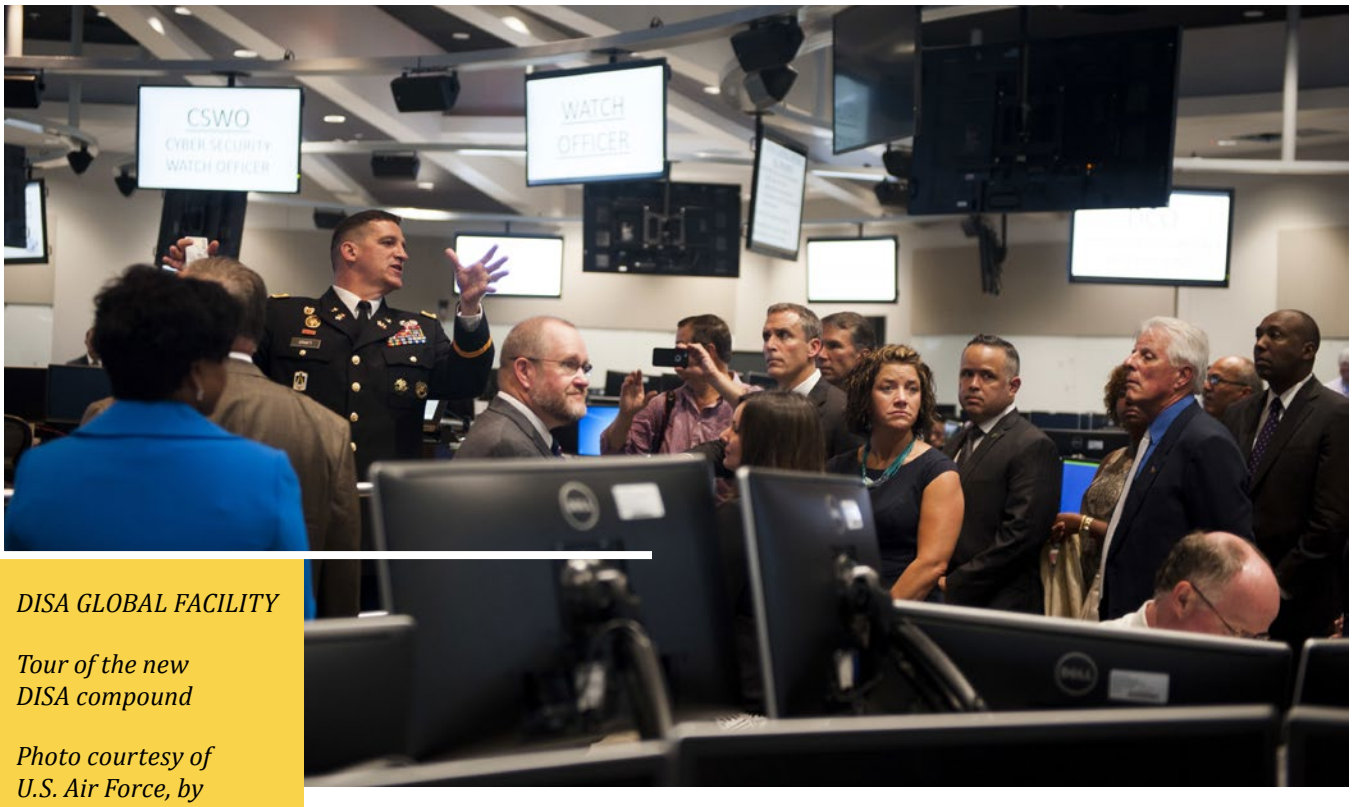
The DoD Cyber Mission Force, U.S. Cyber Command, and the Military Services have identified a strategy to build, develop, and increase the number of professions with unique skills to perform critical functions such as computer network defense. The strategy generally entails developing and using new military occupational specialties, ratings and designators within the Military Services, training and career development paths, and retention options to bolster critical skills and improve the cyber workforce.

The DoD Cyber Mission Force, U.S. Cyber Command, and the Military Services have identified a strategy to build, develop, and increase the number of professions with unique skills to perform critical functions such as computer network defense.

The DoD OIG issued a classified report in 2015 concluding that the Services faced continued challenges in fielding Cyber Mission Force teams. Among other actions, the DoD OIG recommended revising or developing fielding strategies and expanding training capacity to build Cyber Mission Force teams. Since the issuance of that report, the Deputy Secretary of Defense and the Commander, U.S. Cyber Command, stated that the DoD was attracting and recruiting a cyber workforce at a faster pace because of changes that gave the DoD enhanced authority to hire critical cyber professionals.

With regard to oversight of information technology systems and building the cyber workforce, the OIG will continue to conduct oversight in this challenging area. In FY 2017, the DoD OIG has ongoing or planned audits that will determine whether the:

- National Security Agency implemented appropriate controls to protect its systems, networks, and data from insider threats;
- combatant commands integrated offensive and defensive cyberspace operations into command plans;
- U.S. Cyber Command and the Military Services integrated the National Guard and Reserve Components in the Cyber Mission Force;
- Military Services and Defense Information Systems Agency effectively implemented Joint Regional Security Stacks as part of its Joint Information Environment initiatives;
- Army secured electronic health records;
- DoD Components developed and tested contingency plans to minimize disruptions to operations;
- Military Services implemented approved and secure physical access control systems at DoD facilities and installations; and
- DoD effectively and appropriately shared cyber threat indicators within the Federal government.



DISA GLOBAL FACILITY

Tour of the new DISA compound

Photo courtesy of U.S. Air Force, by Staff Sgt. Clayton Lenhardt/Released

In sum, although the DoD has taken steps to increase cybersecurity through offensive and defensive operations and build its Cyber Mission Force, significant challenges remain. The DoD needs to continue to focus in areas such as maintaining a skilled cyber workforce, developing and using cyber capabilities, and integrating cyberspace operations into command plans. The challenge for cybersecurity is that adversaries and defenders constantly innovate and adapt capabilities, and it is a continuous effort to protect DoD's systems and networks from increasingly sophisticated cyberattacks. The DoD must develop and evolve its tactics, techniques, and technology and build and retain a highly skilled cyber workforce to detect and respond to increasingly sophisticated threats, whether defensively or offensively.

FINANCIAL MANAGEMENT

Equipment procurement decisions are better justified when supported by reliable financial and managerial information.

Photo courtesy of U.S. Air Force, Senior Airman Justyn M. Freeman

the Challenge—#5

Improving Financial Management

Financial management challenges continue to impair the DoD's ability to provide reliable, timely, and useful financial and managerial information to support operating, budgeting, and policy decisions. DoD financial management covers a complex array of financial topics—including procurement, inventory, payroll, asset management, and real property—across a very complex organization structure. However, the DoD is the only Federal agency that has never undergone a full financial statement audit. Moreover, the DoD financial statements are the major impediment to a successful audit of the U.S. Government.

The DoD financial statements have not been ready for audit since the DoD began preparing financial statements in the early 1990s. Neither the DoD as a whole nor its Military Services have been able to provide auditors sufficient evidence to undergo a financial statement audit.

The DoD is required by the Chief Financial Officers Act of 1990 to achieve a full financial statement audit covering its budget, assets, and liabilities. Public Law 111-844 specifically requires DoD to have audit-ready financial statements by September 30, 2017. In addition, the Office of Management and Budget Circular No. A-123 defines management's responsibilities for enterprise risk management and internal control. The Circular emphasizes the need to integrate and coordinate risk management and strong and effective internal controls into existing business activities and as an integral part of managing an agency. Enterprise risk management is a key element of reaching financial auditability and the DoD continues to be challenged by these requirements.

Financial Auditability

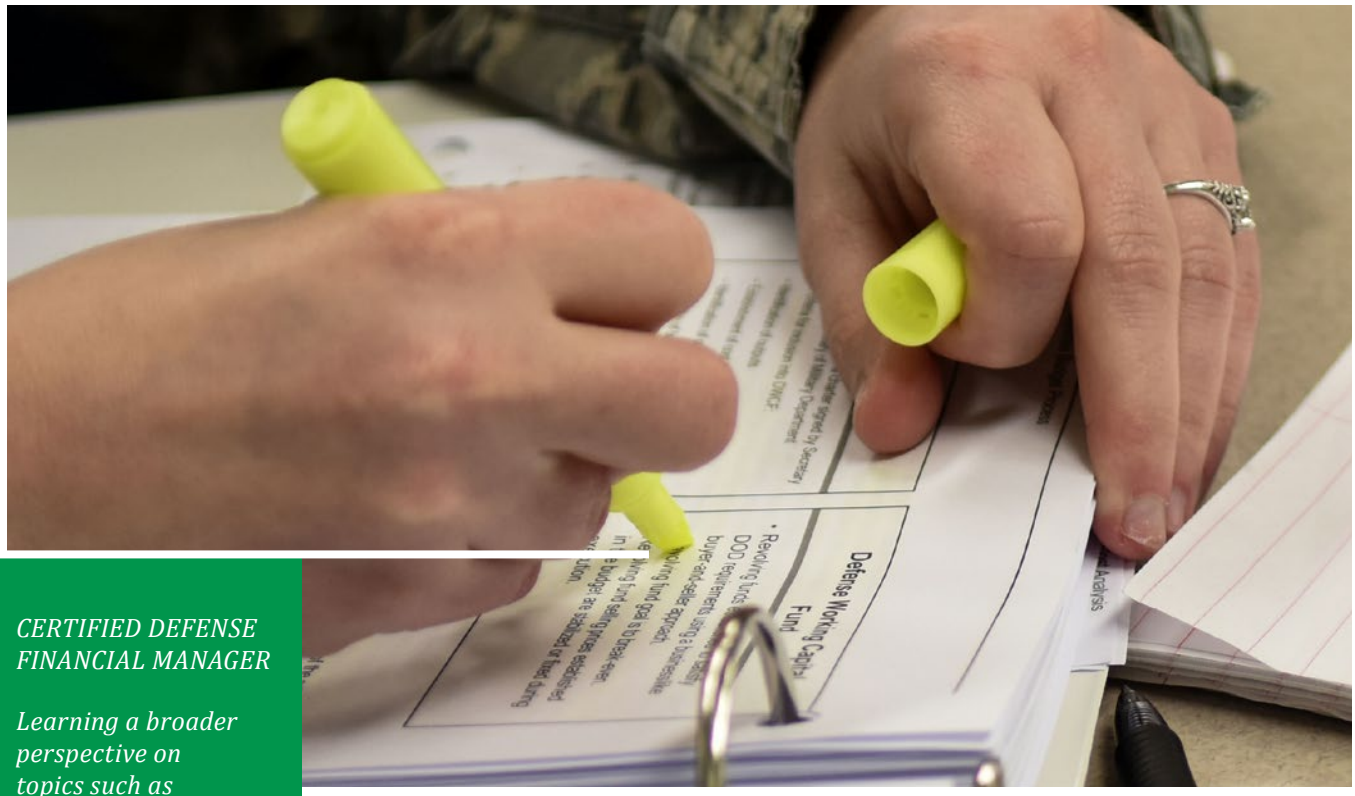
Providing auditable financial statements is critical for ensuring that programs are working and funds are being used properly. Unreliable financial information makes it difficult to accurately develop and execute budgets or to determine the effectiveness and efficiency of military operations. DoD financial management challenges make it difficult to see potential waste, mismanagement, and cost overruns. Financial management procedures are often manual and limit the DoD's ability to develop repeatable processes that could be achieved through well-designed automated solutions.

Unreliable financial information makes it difficult to accurately develop and execute budgets or to determine the effectiveness and efficiency of military operations.

If the DoD can achieve a favorable opinion on its financial statements, these improvements can also help management make better decisions when predicting operational requirements. For example, the DoD OIG found that some budget submitting offices in the Navy could not support the validity and accuracy of obligations during its triannual review of unliquidated obligation and unfilled customer orders in May 2014. This inability to support the obligations did not provide the Navy with the assurance that its financial reporting accurately reflected the status of its obligation and may have lost the opportunity to use funds for other purposes.

Current State of Audits

DoD OIG audits continue to show a lack of supporting documentation for account balances and system data that are not reliable, accurate, or timely. Asset information, such as inventories, continues to show problems with valuation, location, and counts that can result in operations placing orders for new parts or equipment even though there are sufficient supplies on



CERTIFIED DEFENSE FINANCIAL MANAGER

Learning a broader perspective on topics such as auditing, accounting, acquisitions, finance and certifying.

Photo courtesy of U.S. Air Force, Airman Shawna L. Keyes

hand. Lack of well-designed system interfaces also hamper the DoD's ability to compile accurate and timely financial and program information. For instance, the DoD OIG has found that the DoD lacks adequate internal controls over the disbursement and obligation of appropriated funds, key reconciliations to "balance the checkbook," appropriately valuing its assets, improving controls in key financial systems, and preparing unsupported journal vouchers used to force accounting entries in the financial statements to match. The DoD OIG's July 2015 audit report summarizing prior audits of DoD financial management highlighted these material internal controls weaknesses and identified that the corrective action for over 130 recommendations still needed to be implemented. Some recommendations were over 4 years old.

The DoD OIG also performed a series of audits on improvements needed in DoD's management of suspense accounts. These suspense account audits highlighted that the DoD could not account for all of its transactions on the DoD's financial statements. Suspense accounts are designed to temporarily hold funds that belong to the Federal Government that do not have enough accounting information to immediately post the transaction to the proper financial statement. However, DoD did not have controls in place to accurately record suspense account balances on the proper component-level financial statements or clear suspense account transactions and

incorrectly recorded collections from revenue-generating programs, service member tax withholdings. In July of 2016, the DoD OIG reported that the Army did not adequately support trillions of dollars in journal voucher adjustments on its FY 2015 financial statements and that it materially misstated its inventory by millions of dollars. The value of unsupported journal vouchers continue to limit the reliability of the financial accounting information for decision makers who need to know whether programs are working and funds are being used properly. Inaccurate inventory information also limits DoD's ability to ensure materiel and equipment is available to for operational readiness.

In July of 2016, the DoD OIG reported that the Army did not adequately support trillions of dollars in journal voucher adjustments on its FY 2015 financial statements and that it materially misstated its inventory by millions of dollars.

Corrective Actions Taken by the DoD

Although DoD plans to conduct its full financial statement audits beginning October 1, 2017, as required by law, several key challenges continue to face the DoD when preparing for the audits. To address these challenges, the DoD is leading enterprise-wide initiatives that seek to support audit readiness or improve overall financial management. The DoD continues to update the Financial Management Regulation and issue policy memorandum to implement accounting policies and better ensure sustainable, repeatable, and standard processes. It also established formal governing bodies to emphasize the importance of DoD business and financial operations and achieving audit readiness. The DoD has also created working groups to ensure that solutions to its financial impediments comply with accounting standards and can pass auditor testing. DoD leaders are closely monitoring its progress.

What is Left to Do – Auditor's Perspective

Achieving audit readiness by September 30, 2017, will be a difficult challenge. These challenges cut across DoD Components and require DoD-wide changes to policies, procedures, and regulations. The major impediments to auditability require the DoD to improve and in some cases change its way of doing business. Long-standing business processes that have supported DoD missions are not always sufficient for an audit and must be transformed. For example, audits conducted by independent public accounting firms of the Services' FY 2015 Schedule of Budgetary Activity cited more than 700 combined findings and recommendations that revealed individual and systemic issues that resulted in unfavorable opinions on the Schedules. Correcting material weaknesses and significant deficiencies that have been identified by public accounting firms should be the first priority

of the Military Services. The DoD also needs to develop sustainable and repeatable processes to better respond to audit requirements and provide the best supporting documentation for sampled transactions.

To achieve and sustain audit readiness, the DoD must also focus on its high-risk areas such as the ability to eliminate the use of journal vouchers as a means of addressing unsupported accounting transactions. The DoD should also consider further consolidating the financial management systems throughout the DoD. The sheer number of business and financial systems is staggering when compared to other Federal agencies, and the level of effort and cost of ensuring all systems are audit ready is significant. DoD needs to expedite the retirement of legacy systems and ensure that remaining systems are interfaced appropriately. These systems should capture and process timely and accurate financial and program data that decision makers can rely upon to ensure programs are working and funds are being used properly.

Because the financial management processes lack adequate controls to support such a complex and convoluted structure they must eliminate systems and continue to develop and document adequate controls that comply with accounting standards.

The DoD's financial management environment is decentralized and consists of hundreds of systems processing transactions reported in the financial statements. Because the financial management processes lack adequate controls to support such a complex and convoluted structure they must eliminate systems and continue to develop and document adequate controls that comply with accounting standards.

Achieving audit readiness and improved financial statements requires leadership focusing attention on this effort. In this effort, leaders across the DoD are communicating that audit readiness remains a DoD-wide priority. Secretary Carter and Deputy Secretary Work continue to emphasize the importance of improving DoD business and financial operations and achieving audit readiness. The DoD are also monitoring progress. For example, in March 2016, a senior leadership committee co-chaired by the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff reviewed the status of audit readiness. Each Military Department reported it was on track to be ready for an audit by September 30, 2017. The Deputy Secretary stressed the importance of making and sustaining improvements.

Yet, while the DoD plans to have 90 percent of DoD's total budgetary resources and 43 percent of total assets under audit in FY 2017, there are still critical capabilities and remediation efforts that need to be accelerated in order for full financial statement audits to begin in FY 2018. Further, the DoD needs to address how to protect sensitive data while still

presenting financial statements in compliance with U.S. Generally Accepted Accounting Principles. These challenges are magnified as the DoD is also facing continuous personnel and budgetary constraints as another fiscal year begins under a continuing resolution.

In addition, the DoD must be able to account for its assets reported on its Balance Sheet, including adequate support for how much assets cost, how much the DoD owns, and where the assets are located. In addition, audit success is closely linked to cash traceability, including proper management and accountability of all transactions to include fully reconciling financial transaction universes. Unsupported journal vouchers and unresolved differences between DoD and the Department of the Treasury are material and jeopardize achieving audit ready financial statements.

Without these improvements, the DoD financial statements will continue to remain unreliable and managers will not be able to rely on its accounting systems to make important management and resource decisions.

Without these improvements, the DoD financial statements will continue to remain unreliable and managers will not be able to rely on its accounting systems to make important management and resource decisions.

Improper Payments

Improper payments are defined as payments, including both overpayments and underpayments, that should not have been made or that were made in an incorrect amount. Reducing improper payments is another important financial management challenge facing the DoD. Improper payments are often the result of unreliable data or a lack of adequate internal controls that increase the likelihood of fraud.

Recently, DoD OIG reports highlighted improper payments related Government travel charge cards. For example, in March 2016, the DoD OIG reported that the DoD Components did not take adequate actions to reduce estimated improper payments in the DoD Travel Pay program, as required by the Improper Payments Elimination and Recovery Act (IPERA). The DoD OIG reported that the DoD missed its improper payment reduction goals for 3 consecutive years. In addition, the GAO reported in June 2016 that the DoD did not submit proposals for reauthorization or statutory changes to Congress in response to 3 consecutive years of noncompliance with IPERA requirements in its Travel Pay program.

For the DoD FY 2015 Agency Financial Report, the DoD met five of the six requirements in accordance with the IPERA. Specifically, the DoD published a financial report; conducted program-specific risk assessments; published corrective action plans; published improper payment estimates; and reported improper payment rates of less than 10 percent. However, the DoD did not achieve its improper payment reduction targets for one of the eight payment programs with established targets. Not attaining reduction targets indicates that additional corrective actions are needed to reduce improper payments.

Overall, the DoD OIG found that the DoD has made progress in improving the identification and reporting of improper payments. For example, it has taken corrective actions to implement recommendations made by the DoD OIG to reduce improper payments in the DoD Travel Pay program and complying with IPERA, such as submitting remediation plans to address internal control deficiencies, and developing metrics and quality assurance goals related to IPERA reporting.

An August 2016 report found that DoD management and travel card officials did not take appropriate action when notified that cardholders potentially misused their travel card.

Additionally, two recent DoD OIG reports identified challenges with improper payments related to Government travel credit cards. A May 2015 report found that from July 1, 2013, through June 30, 2014, DoD cardholders had 4,437 transactions totaling $952,258, where they likely used their travel cards at casinos for personal use. In addition the DoD OIG identified 900 DoD cardholder transactions totaling $96,576 at adult entertainment establishments. An August 2016 report found that DoD management and travel card officials did not take appropriate action when notified that cardholders potentially misused their travel card. Specifically, DoD management did not perform reviews on sampled cardholders, did not take action to eliminate additional misuse, and did not review cardholder travel vouchers that indicated personal use. By reducing improper payment, DoD can use those funds to meet other critical operational needs.

GREEN ENERGY

The William A. Jones III building on Joint Base Andrews, Md., is a Leadership in Energy and Environmental Design certified building. It features approximately 48,000 square feet of environmentally friendly green roof space.

Photo courtesy of U.S. Air Force, Airman 1st Class Rustie Kramer

the Challenge—#6

Protecting Key Defense Infrastructure

Protecting key defense infrastructure, such as installations, space, and the defense industrial base, is a critical challenge for the DoD. The DoD must ensure that its installations worldwide are protected and sustained to meet operational mission requirements. The DoD must also maintain and protect its assets in space. In addition, the DoD needs to address supply chain vulnerabilities and its strategic competitors.

Installations and Energy

The DoD manages over 500 installations worldwide, consisting of nearly 300,000 buildings. It must ensure that each installation is maintained and sustained to support operational mission requirements. To accomplish this, the DoD is constantly prioritizing its military construction, sustainment, and recapitalization requirements. The DoD must meet these requirements, with constrained funding, while managing the security risks to installations and the challenge to contribute to mission readiness.

The growing need for military construction projects has increased the need for accurate and reliable justifications and cost estimates for military construction projects. The DoD has made progress in managing installations efficiently and economically. In particular, the DoD has increased the use of renewable energy and energy saving projects on DoD installations to provide energy security and to help the DoD comply with various energy mandates and goals. Some of the renewable energy and energy saving projects include improved lighting; high-efficiency heating, ventilation, and air conditioning systems; double-pane windows, solar and wind electricity, and new roofs.

In FY 2015, the DoD spent $16.7 billion to satisfy the DoD's energy needs. However, OIG audits show that DoD has not implemented sufficient controls to effectively monitor and oversee renewable energy and energy contracting. Specifically, a series of audits demonstrated that DoD does not have sufficient programs to ensure that energy savings performance contracts and utility energy services contracts were providing cost savings. In some cases, the DoD spent millions on projects that may not have achieved sufficient energy savings to pay back the utility company's investment as required or to support payments to the contractor based on estimated guaranteed future annual cost savings.

In addition, energy availability directly affects the capabilities of weapons platforms, facilities, and equipment, while remaining a substantial expense for the DoD. Energy is an important part in sustaining worldwide military operations because energy is used by installations, ships, aircraft, and combat vehicles. Some of the DoD's largest challenges are supporting energy innovation in current operations and integrating energy considerations into force development. Furthermore, the DoD is striving to meet the President's goal to produce or procure not less than 25 percent of its total energy consumption from renewable sources by 2025.

A series of audits demonstrated that DoD does not have sufficient programs to ensure that energy savings performance contracts and utility energy services contracts were providing cost savings.

NEXT GENERATION LAUNCH VEHICLES

The Vulcan launch system is being developed by ULA and will replace the Delta IV Heavy launch vehicle (pictured above)

Photo courtesy of NASA, Kim Shiflett

Space

The DoD's assured access to space and its ability to maintain space control is a significant management challenge. Space control seeks to support freedom of action in space and, when necessary, defeat adversary efforts that interfere with or attack U.S. or allied space systems and negate adversary space capabilities.

Currently, with regard to assured access to space, the Air Force is attempting to reduce the cost of national security launches and eliminate the reliance on Russian-made RD-180 engines. To accomplish these objectives and to move to a new generation of launch vehicles, the Air Force must certify two new launch vehicles being developed by the United Launch Alliance (ULA) and Space-X. In addition to access to space, the DoD needs to maintain the long-term dominance of its space technologies and capabilities. In September 2016 testimony before the Senate Armed Services Committee, for example, General Hyten emphasized the importance of operations in space, "In space, threats continue to grow… as potential adversaries attempt to counter what has become a critical advantage for our Nation and our allies."

Recent OIG space-related projects include ongoing quality assurance inspections of ULA and Space-X launch vehicle manufacturing and test operations. The OIG plans to conduct other space-related oversight projects in the future.

Defense Industrial and Technology Base

The DoD draws from a large network of global suppliers for its equipment and support needs. For example, in fiscal year 2014, the DoD managed over 4.7 million parts that are used in communications and weapon systems, at a cost of over $96 billion. In many cases, this has allowed U.S. firms to harness the creativity of the global market. However, these supply chains create vulnerabilities and are subject to manipulation by strategic competitors.

One of the vulnerabilities within the global supply chain is the widespread existence of counterfeit parts. Counterfeit parts can, for example, delay missions, affect the integrity of systems, and ultimately endanger the lives of service members. Almost anything is at risk of being counterfeited, including microelectronics used in fighter jets and missile guidance systems, fasteners used in aircraft, and materials used in engine mounts.

In response to this risk, in 2013, the DoD created policy to prevent the introduction of counterfeit into the supply chain, as well as testing and other means by which to detect counterfeit materials that may have already entered it. The DoD also issued regulations, as required by the 2012 National Defense Authorization Act, that require DoD personnel and contractors to report suspected counterfeit electronic parts to a cooperative activity between Government and industry. Called the Government-Industry Data Exchange Program, this program allows Government and industry participants to share information on nonconforming parts, including suspect counterfeit parts, through a web-based database. The act also requires that contractors develop and maintain systems to detect and avoid counterfeit electronic parts.

The Government-Industry Data Exchange Program allows Government and industry participants to share information on nonconforming parts, including suspect counterfeit parts, through a web-based database.

The GAO recently reviewed DoD's efforts to address vulnerabilities to counterfeit parts in its supply chain. The GAO found several aspects of DoD's implementation of its mandatory reporting for suspect counterfeit parts have limited its effectiveness as an early warning system. The GAO also concluded that, without proper oversight ensuring that the reporting requirement was consistently applied, the DoD could not ensure it is effectively managing the risks associated with counterfeit parts.

Investigation of product substitution, including counterfeit, defective or substandard products, is one of the top investigative priorities of the DCIS. Product substitution disrupts readiness, wastes economic resources, and threatens the safety of military and Government personnel and other end users. As of September 30, 2016, the DCIS had 159 active product substitution cases that represented approximately 10 percent of active investigations. In FY 2016, the DCIS' product substitution investigations resulted in 5 arrests, 17 criminal charges, 11 convictions, and over $41 million in recoveries for the Government.

A recent DCIS product substitution investigation led to the conviction of an individual, who imported thousands of counterfeit integrated circuits from China and Hong Kong and resold them to U.S. customers, including contractors who supplied them to the DoD for use in nuclear submarines.

A recent DCIS product substitution investigation led to the conviction of an individual, who imported thousands of counterfeit integrated circuits from China and Hong Kong and resold them to U.S. customers, including contractors who supplied them to the DoD for use in nuclear submarines. The perpetrator pled guilty to conspiring to traffic in counterfeit military goods, and was sentenced to 37 months imprisonment, and ordered to pay $352,076 in restitution to the 31 companies. In addition, the perpetrator was issued two forfeiture money judgments totaling over $1.8 million. A separate DCIS investigation found that a company supplied nonconforming mechanical parts to the Defense Logistics Agency for use on various weapons systems, including aircraft, vessels, and vehicles. The majority of these parts were critical application items, which are items essential to weapon system performance or operation, or the preservation of life or safety of operating personnel. A jury convicted the company's president of mail fraud and false claims. The individual is awaiting sentencing and was debarred, along with the company, from Government contracting for a period of 3 years.

In summary, the DoD has made progress in installation and energy management, and it has recognized the urgency of maintaining control of space. It must also focus on preventing the introduction of counterfeit parts in the supply chain, which is a difficult and widespread challenge.

PORT LOOKOUT WATCH

USS George H. W. Bush is underway conducting routine training qualifications in preparation for and upcoming deployment.

Photo courtesy of U.S. Navy, Mass Communication Specialist 1st Class Sean Hurt/Released

the Challenge—#7

Developing Full Spectrum Total Force Capabilities

Designing, building and posturing a total force, active and reserve, capable of executing a wide range of missions across the full spectrum of potential conflict is a continuous challenge for the DoD. Increasingly diverse threats and capability requirements combined with significant budget pressure requires the DoD to make difficult strategic choices in developing its total force.

THIRD OFFSET STRATEGY

Airmen preform maintenance on an MQ-9 Reaper.

Photo courtesy of U.S. Air Force, Airman 1st Class Kristan Campbell/Released

For much of the last decade, the DoD has focused on capabilities needed for combatting violent extremists and building partner capacity in Afghanistan, Iraq, and, most recently, Syria. As noted in previous challenges, violent extremism and terrorism continue to threaten the United States and its allies. At the same time, Russia, Iran, North Korea, and China are threatening U.S. strategic interests and the stability of regions throughout the world. Other countries and non-state actors continue attempts to obtain and upgrade modern conventional weapons, advanced technologies, and weapons of mass destruction.

As the DoD builds on the new capabilities it has developed in the fight against violent extremists, it also must refocus on capabilities necessary to counter current and future strategic threats. This refocus extends across all domains (land, sea, air, space, and information) and heightens competition for resources, the need for new ways of thinking to extend U.S. military dominance, and the critical importance of optimizing the value of DoD capabilities and components across the full spectrum of conflict.

The most recent DoD initiative to maintain U.S. military superiority over its adversaries, primarily China and Russia, is its Third Offset Strategy. Announced in FY 2015, this strategy seeks to develop and employ new technologies and operational concepts to offset adversaries' investments while increasing U.S. capabilities in a way that it cost effective. With its

emphasis on research and development, experimentation, war gaming, and faster adoption of new technologies, the Third Offset Strategy is a timely and promising initiative that will benefit from OIG oversight.

DoD is reviewing how it will train and use Active and Reserve Components and where to position its personnel and assets throughout the world to ensure it has adequate total force capability.

In addition to pursuing innovative technologies and operational concepts, the DoD continues to assess the size and mix of its total force to maintain an optimal mix of active and reserve forces that can defeat our enemies and defend the homeland. For example, the DoD is reviewing how it will train and use Active and Reserve Components and where to position its personnel and assets throughout the world to ensure it has adequate total force capability. This is not a new issue. In 2007, the Secretary of Defense wrote that the DoD was assessing options on how best to support global military operational needs, including whether the DoD has the right policies to govern how Reserve, National Guard, and Active Component units are used. In 2008, the Secretary issued guidance emphasizing that the Reserve Components provide operational capabilities and strategic depth to meet U.S. defense requirements across the full spectrum of conflict and that the military services need to better integrate Reserve Component capabilities into their respective total force structures. The Services efforts to assess the right balance of active duty, reserve, and National Guard resources are discussed below.

In May 2011, the Secretary of the Air Force discussed reshaping the structure of the Air Force in the face of enduring budget constraints. At that time, the Air Force had 144 initiatives across the service aimed at identifying efficiencies and the right mix of personnel, technology, and modernization. In 2014, Congress also established the National Commission on the Structure of the Air Force to recommend how the force structure should be modified to meet present and expected mission requirements within available resources. The Commission's report, issued in January 2014, provided recommendations to rebalance Active, Reserve, and Air National Guard components; increase the end strength of the Reserve components; and increase regular, periodic, and predictable use of Reserve component forces.

The National Commission made recommendations to increase the number of "associate units" between Active and Reserve components and to create a single integrated chain of command for these associate units. Acting on these recommendations in the report, the Air Force intends to reach initial operational capability in its Integrated Wing Pilot Program in FY 2017. This program will align Active and Reserve components under a single chain of command to leverage the strengths of both components and meet mission requirements more efficiently and effectively.

The FY 2015 National Defense Authorization Act established the National Commission on the Future of the Army to evaluate, in part, how Army National Guard and Army Reserve personnel are integrated into the Total Force. DoD and Army policy directs the Army to ensure total force policies encourage the optimum use of active and reserve component personnel and to organize, man, train, and equip the Army, Army National Guard, and Army Reserve as "an integrated, operational Total Force." During a speech on August 3, 2016, the Secretary of Defense stated, "The days of the National Guard serving exclusively as a strategic reserve are over." He added that the Guard is an "indispensable component of the Total Force," whether in day-to-day activities or large-scale operations. Army National Guard officials acknowledge that this new role will require a shift in the mindset of Guard unit leadership and personnel.

As part of a series of audits on the readiness of military units, the DoD OIG is completing an audit of National Guard Armored Brigade Combat Teams training to perform unified land operations—a full spectrum operations capability. Based on interim audit results, the DoD OIG issued a Notice of Concern to the Army National Guard regarding turnover within key leadership positions and methods used to assess and report readiness for some units. The DoD OIG also determined that training programs were not effective in ensuring whether units could attain and sustain mission proficiency. The DoD OIG recommended that the Army and the Army National Guard provide commanders clear guidance for managing training programs, maintaining unit cohesion, and ensuring assessments more accurately reflect training readiness.

During FY 2017, the DoD OIG will conduct an audit of personnel readiness reporting levels in National Guard units. Personnel readiness data, such as the type, number, rank, and status of personnel assigned to a unit, is critical information that leaders need to make informed decisions on whether units are available to deploy. As the role of the reserve components in DoD's total force continues to evolve, DoD's ability to rely on personnel readiness data provided by the Guard units will become increasingly important. The planned audit will focus on accuracy of reported personnel readiness levels at select Army National Guard and Air National Guard units.

Personnel readiness data, such as the type, number, rank, and status of personnel assigned to a unit, is critical information that leaders need to make informed decisions on whether units are available to deploy.

The Navy is increasing its fleet from 280 ships at the end of FY 2016 to 308 ships in FY 2021. The fleet consists of aircraft carriers, submarines, surface combatants, amphibious ships, combat logistics ships, and support ships. The Navy's top shipbuilding priority is to replace the aging Ohio

class ballistic missile submarines, which are a key component of the nation's nuclear triad. The Navy plans to build the first new Ohio-class submarine in FY 2021. Additionally, although the Navy is statutorily required to maintain 11 aircraft carriers, it has operated 10 carriers since the retirement of the USS Enterprise in 2012. Extended deployments of the remaining ships have placed stress on crews. The critical and costly carrier and submarine programs consume about half of the Navy's shipbuilding resources, affecting the Navy's ability to build ships of other classes. The Navy has identified additional amphibious vessel requirements and has a significant shortfall in small surface combatants. While prioritizing shipbuilding, the Navy is also taking steps to improve information warfare capabilities, invest in naval aviation, rapidly integrate unmanned systems, and bolster investments in advanced weapons. Filling capability gaps while maintaining the current fleet and meeting global operational and forward presence requirements is a significant management challenge for the Navy that requires objective oversight.

The critical and costly carrier and submarine programs consume about half of the Navy's shipbuilding resources, affecting the Navy's ability to build ships of other classes.

Regarding force size, the DoD's FY 2017 budget request includes a total force of 2,073,200 active, reserve, and guard soldiers. The following table shows the total force requests for each service in FY 2017.

Table. DoD Total Force Request for the FY 2017 Budget

	Army	Navy	Marine Corps	Air Force
Active	450,000	323,100	182,000	317,000
Reserve	195,000	58,900	38,500	68,500
Guard	335,000	-	-	105,200
Total	980,000	382,000	220,500	490,700

This force size, the smallest in decades, increases the need for effective management, as well as comprehensive oversight to ensure the most effective and efficient employment of the total force.

For over 50 years, U.S. airpower superiority has been a core component of our full-spectrum total force capabilities. Each Military Service is experiencing challenges in maintaining air combat power advantage over our adversaries. After 25 years of near constant combat and use, DoD's fleet of aircraft is aging and in need of overhaul or replacement. Military aviators remain heavily engaged around the world, yet full-spectrum readiness and the size of the force remain a significant

concern. To address these challenges, the DoD is acquiring new aircraft such as the MV-22 and the F-35 Joint Strike Fighter, as well as slowing the retirement of aircraft like the F/A 18 and A-10 through overhaul and sustainment efforts.

In 2013, the Army began its Aviation Restructuring Initiative in which it planned to cut its aviation force to achieve end-strength and budget-driven structure limitations. The initiative proposed to retire or reassign aircraft and deactivate aviation brigades. The goal of the Army's Aviation Restructuring Initiative is to protect modernization efforts and optimize the mix of Active and Reserve components. For example, the initiative transfers the Apache Helicopters from the Guard to active duty units and reassigns the H-60 from the active duty units to the Guard. In September 2016, the DoD OIG began an audit of the Army's modernization efforts related to the H-60 Black Hawk fleet.

Aging aircraft also has an impact on the training readiness of the aviators who have less equipment on which to train. In March 2016, the Senate Armed Services Committee specifically expressed concerns about whether Marine Corps aviators were conducting sufficient training and if squadrons had the appropriate number of aircraft to maintain training readiness and respond in crisis. As part of an ongoing series on the readiness of military units, the DoD OIG has initiated an audit to assess whether Marine Corps aviation squadrons have adequate aircraft capable of performing assigned missions and sufficient trained aviators to meet readiness requirements.

In March 2016, the Senate Armed Services Committee specifically expressed concerns about whether Marine Corps aviators were conducting sufficient training and if squadrons had the appropriate number of aircraft to maintain training readiness and respond in crisis.

The DoD's efforts to improve active and reserve integration provide depth that increases the DoD's ability to protect U.S. interests in regions throughout the world such as the Asia-Pacific Region. In 2011, President Obama called for the United States to return its attention to the Asia-Pacific region and called for a rebalancing of forces in the area. In 2015, Secretary Carter stated that the DoD's roles in the Asia-Pacific rebalance are to:

- invest in future security capabilities such as a new long-range stealth bomber, a long-range anti-ship cruise missile, and rapid runway repair;
- field capabilities—like the Virginia-class submarine and F-35 Joint Strike Fighter—developed over the last decade for use in the region;
- leverage new uses for existing technologies such as adapting the Tomahawk from a fixed, land-based target environment to use in a mobile maritime environment;

READINESS TRAINING

MV-22 Osprey used in support of tactical recovery training.

Photo courtesy of U.S. Marine Corps, Cpl. Trever Statz/Released

- adapt regional force posture to include the construction of new facilities and geographic distribution of equipment and personnel across the region; and
- reinforce alliances and partnerships through efforts such as security and technology cooperation and humanitarian and disaster relief.

To determine if units are equipped to execute their missions, the DoD OIG has audited the distribution of equipment across the Asia-Pacific region. Specifically, the DoD OIG conducted multiple audits on the ability of Military Services to effectively equip their units in the region. For example, the DoD OIG recently conducted a series of munitions inventory audits in the region to determine whether the Navy and Air Force had an accurate account of the type, quantities, and condition of its munitions. Two additional DoD OIG audits determined that Army and Marine Corps units in Korea did not have sufficient, properly maintained chemical-biological personal protective equipment and that units were not training to conduct operations under appropriate threat conditions. In FY 2017, DoD OIG will conduct a followup audit to determine whether Air Force commands have implemented corrective actions related to a 2013 DoD OIG audit on the stocking and distribution of expeditionary airfield resources and repair kits. These audits demonstrate that the U.S. Pacific Command preparedness for contingency operations remains a challenge.

In addition, the DoD is transferring defense equipment to its international partners to enhance their military capabilities and enable their military forces to work with U.S. forces in deterring and defeating aggression. Under the Foreign Military Sales Program, the DoD sells advanced defense equipment, such as unmanned aircraft systems and radar systems, to international partners and conducts post-delivery monitoring to ensure transferred equipment is used for intended purposes established in international agreements. The DoD OIG recently announced the first in a series of audits to evaluate DoD's oversight of U.S. defense equipment transferred to international partners in the Asia-Pacific region. The audit will determine whether U.S. Pacific Command is conducting its Enhanced End-Use Monitoring Program to ensure that advanced defense equipment transferred to international partners is being used for intended purposes.

The DoD OIG recently announced the first in a series of audits to evaluate DoD's oversight of U.S. defense equipment transferred to international partners in the Asia-Pacific region.

The DoD IG, as the Chairperson of the of the Interagency Coordination Group of Inspectors General for the Guam Realignment, issues an annual report on the programs and operations on Guam funded with military construction appropriations. The annual report also summarizes oversight efforts of the DoD OIG, the Department of the Interior, and the Service-level audit agencies related to these funds. In addition to its role on the Interagency Coordination Group, the DoD OIG also continues to provide oversight through audits related to the realignment. For example, in 2015, the DoD OIG reviewed the administration of the Guam Multiple Award Construction Contract, a $4 billion contract issued by the Navy for military construction projects related to the relocation of Marines to Guam. The report identified weaknesses in the Navy's contract administration processes, which led to the construction of facilities that did not meet mission and regulatory requirements.

Where forces are deployed throughout the world is another critical issue for maintaining full-spectrum total force capabilities. Evolving threats throughout the world, as discussed previously, affect these key strategic decisions. For example, in recent years, the U.S. and NATO allies across Europe are increasingly challenged by political instability in the region, often spurred by Russia. However, following the dissolution of the Union of Soviet Socialist Republics and the Warsaw Pact, the DoD reduced its force posture and closed bases in Europe. In light of recent conflicts and instability, the DoD has committed to supporting U.S. interests and allies in the region through increased presence and multinational training events and exercises.

From FY 2015 to FY 2017, the DoD budgeted nearly $5.2 billion to fund the European Reassurance Initiative. Through the initiative, the DoD seeks to reassure our NATO allies and bolster the security and capacity of our partners. The initiative consists of increasing the presence of U.S. forces in Europe through stepped-up rotations and continued deferral of some previously planned force reductions or potential force restructuring initiatives. Specifically, the Army is augmenting its presence through the rotation of stateside units. The Air Force is sustaining its current air superiority force structure in Europe and augmenting NATO's Baltic Air Policing mission. The Navy will continue its expanded presence in the Black and Baltic Seas.

To assess the effect of this initiative, in April 2016, the DoD OIG initiated an assessment of the effectiveness of the European Reassurance Initiative. This assessment will evaluate, among other matters, whether improvements have been made to European partner country infrastructure and whether U.S. and NATO forces have increased force responsiveness, interoperability, and sustainability. The DoD OIG also recently announced an audit to determine whether the U.S. European Command is integrating offensive and defensive cyberspace operations into its operational and contingency plans.

Adequately training and equipping the force to recognize, respond, operate, and recover from CBRNE attacks and hazards remains a challenge for the DoD and an oversight priority for DoD OIG.

Chemical, Biological, Radiological, Nuclear and Explosive Issues

Countering the potentially catastrophic effects of Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) weapons is a key component to the challenge of maintaining full-spectrum total force capabilities. DoD's challenge in this area is two-fold. The DoD must protect military personnel from CBRNE threats and train them to carry out military operations under CBRNE threats or hazards. The DoD must also ensure proper handling of the CBRNE materials in its possession and protect the public from exposure. Adequately training and equipping the force to recognize, respond, operate, and recover from CBRNE attacks and hazards remains a challenge for the DoD and an oversight priority for DoD OIG.

Hostile actors, including terrorists and supporters of terrorists, are seeking to acquire weapons of mass destruction and materials to construct weapons of mass destruction. This poses a significant and potentially catastrophic threat to the United States and its allies. CBRNE threats include the intentional employment of, or intent to employ, weapons or

CBRNE

A search for chemical or biological agents during site-assessment training.

Photo courtesy of U.S. Army, Sgt. Eliverto V. Larios

improvised devices that produce CBRNE hazards. To counter this threat, the DoD must enable its forces to deter, prevent, protect, mitigate, respond, and recover from CBRNE threats and effects. Achieving this mission requires, in part, equipping the force to successfully conduct military operations under CBRNE threats and effects.

As previously discussed, the DoD OIG recently conducted two audits that identified weaknesses in CBRNE equipment and collective training for Army and Marine units in Korea. Because of concern that similar equipment and training weaknesses may exist in other commands, the DoD OIG intends to assess whether U.S. Special Operations Command has sufficient quantities and types of CBRNE equipment on hand. The audit will also evaluate if personnel are adequately trained and CBRNE qualified.

The DoD OIG is also conducting a series of projects concerning the security of and accountability for CBRNE materials in DoD's possession. In April 2016, the DoD OIG issued a report on the evaluation of controls over biological materials in DoD Component laboratories. The evaluation highlighted weaknesses in the oversight of several DoD laboratories including inconsistent guidance and inspection policies across the Military Services and inadequate training of officials conducting inspections of the facilities. The DoD OIG is also completing an audit that will address the controls over chemical surety materials at DoD installations and

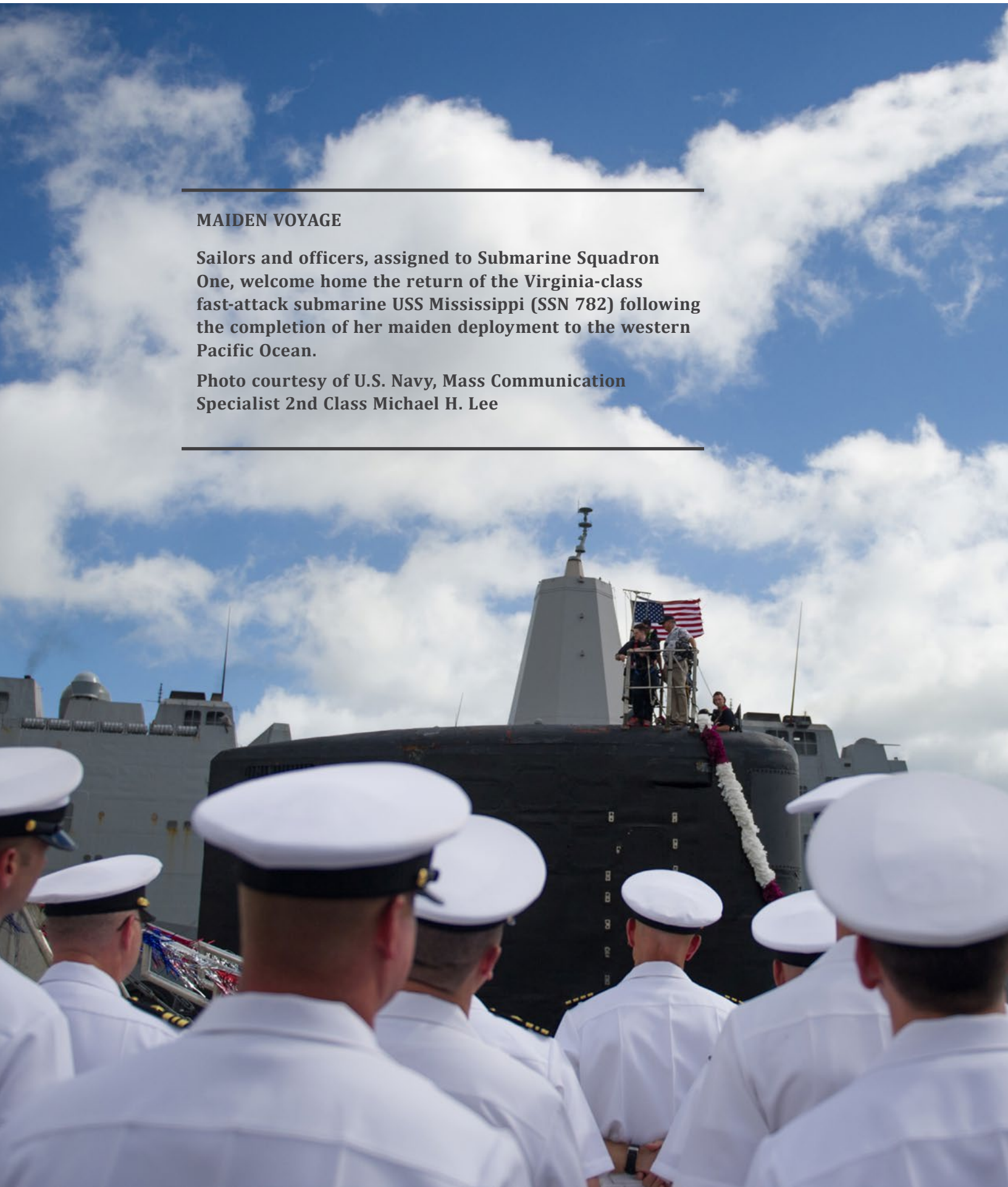
laboratories. The review will address the security controls over these materials including accountability for the chemical agents, access controls to facilities, and vetting of personnel who have access to and protect chemical materials. In 2017, the DoD OIG plans to conduct a review of the Nuclear Surety Program that will review the controls over personnel with access to or responsibility for safeguarding nuclear materials.

In 2017, the DoD OIG plans to conduct a review of the Nuclear Surety Program that will review the controls over personnel with access to or responsibility for safeguarding nuclear materials.

The DoD OIG continues to oversight of the governance and sustainment of the U.S. nuclear weapons enterprise. A 2016 OIG review detailed weaknesses and open recommendations from the last 5 years of DoD OIG nuclear reports, such as weaknesses in guidance for implementing Presidential and DoD directives**,** requirements for nuclear weapon security and employment, manning and training of theater nuclear planners, budget or funding priority to sustain nuclear command and control capabilities, and logistics and parts issues to sustain the Minute Man III missiles. In addition, a September 2016, DoD OIG report documented a lack of interdepartmental coordination on intelligence requirements for the nuclear enterprise.

Other reviews related to DoD's capabilities are ongoing. For example, the DoD OIG is currently reviewing the National Airborne Operations Center's ability to sustain its mission with the E-6B aircraft and evaluating the DoD's ability to organize, train, and equip explosive ordnance disposal teams that support the DoD's nuclear weapons mission. In FY 2017, the DoD OIG plans to examine the availability and reliability of the E-6B program (airborne command, control, and communications), the sustainment of nuclear ballistic missile submarines, and the ability of the nuclear detonation detection system to meet its DoD requirements.

In short, the DoD has recognized the importance of continually assessing and modifying its force structure and capabilities to counter evolving strategic threats, and this effort remains a continuing management challenge, particularly given growing pressure on resources.



MAIDEN VOYAGE

Sailors and officers, assigned to Submarine Squadron One, welcome home the return of the Virginia-class fast-attack submarine USS Mississippi (SSN 782) following the completion of her maiden deployment to the western Pacific Ocean.

Photo courtesy of U.S. Navy, Mass Communication Specialist 2nd Class Michael H. Lee

the Challenge—#8

Building and Maintaning Force Readiness

Building and maintaining the readiness of the current force to execute its diverse missions is one of DoD's core challenges and responsibilities. The DoD must ensure its forces are manned, trained, and equipped to deter and defeat our adversaries and to protect U.S. interests at home and abroad.

The DoD faces the challenge of rebuilding readiness after 15 years of continuous deployment. DoD leaders have stressed the need to balance current readiness against modernization and future force development to ensure forces can prevail against current and future threats. To maintain force readiness, the DoD needs to provide adequate equipment and also ensure the return of costly serviceable equipment from overseas deployments. In addition, the DoD must provide quality health care for members of the Military Services and their families, focus on suicide prevention, and recruit and retain high quality military and civilian personnel.

Equipment Accountability and Reset

An important aspect of readiness is the availability and functionality of the equipment for both training an operational needs. Properly accounting for equipment protects taxpayer money and allows DoD to appropriately and promptly respond to new contingencies worldwide. It also ensures that needed DoD equipment is not left behind, whether it is rolling stock or nonrolling stock. Rolling stock refers to vehicles such as tactical vehicles, ambulances, and wrecker trucks. Nonrolling stock refers to items such as generators, weapons, and radios. After equipment is returned to the United States, it is reset or refurbished so that it can be re-issued to military personnel for training and deployment.

Property accountability has been a continuous challenge for the DoD in both Iraq and Afghanistan.

Property accountability has been a continuous challenge for the DoD in both Iraq and Afghanistan. At its peak in 2012, more than 18,000 pieces of DoD equipment were used in Afghanistan, with limited accountability. As a result, multiple DoD OIG reports documented the loss of hundreds of millions of dollars in equipment, including thousands of sensitive items. For example, a 2014 report concluded that the Army reported accumulated losses of $586.8 million in equipment in Afghanistan for 1 year. An OIG audit also found poor security, limited qualified property accountability experts, and the lack of urgency when reporting inventory losses in a timely manner in Afghanistan. DoD OIG audit reports also recommended improvements to the security and storage of equipment in Afghanistan, Kuwait, and the United Arab Emirates**,** particularly with sensitive items such as communications equipment.

Suicide Prevention

Suicide continues to be a public health concern for America and its military veterans. Historically, the suicide rate was lower in the military than the civilian population. However, in 2008, for the first time, the suicide rate in the Army exceeded the age and gender adjusted rate in the civilian populace and continued to be higher through 2015. Active Component suicides slightly decreased from FY 2014 through FY 2015, but Reserve Component suicides increased. According to recent DoD data, there were a total of 478 suicides in 2015.

The DoD has developed and promoted prevention policies, practices and programs to attempt to reduce military suicide. For example, the Defense Suicide Prevention Office (DSPO) leads working groups of representatives

LOGISTICS READINESS

The Logistics Readiness Squadron at Joint Base McGuire-Dix-Lakehurst ensures those deploying have the correct materials before leaving.

Photo courtesy of U.S. Air Force, Airman 1st Class Terrence Clyburn

from the Services, the Office of the Assistant Secretary of Defense for Health Affairs, and other stakeholders on expanding access to behavioral health care for service members. The DSPO also implemented the DoD Strategy for Suicide Prevention in 2015 that attempts to coordinate suicide prevention efforts across the DoD. For example, the DSPO has published and distributed guides to military family members on suicide warning signs, risk factors, and actions to take in a crisis. DSPO also sponsors research initiatives and training that address gaps in suicide prevention and resilience policies and practices.

In addition, the DoD collaborates with the Veterans Administration to develop suicide prevention and intervention policy. For example, in June 2013 the DoD and Veterans Administration jointly developed the Clinical Practice Guideline, "Assessment and Management of Patients at Risk for Suicide," which recommends best practices for assessing and managing the risk of suicide among active duty military and veterans.

However, shortcomings in DoD suicide prevention efforts remain. A September 2015 DoD OIG report found that DoD lacked a clearly defined governance structure and alignment of responsibilities for the Defense Suicide Prevention Program. In addition, the report identified the lack of clear processes for planning, directing, guiding, and resourcing to

effectively develop and integrate the Suicide Prevention Program within the DoD. In response to DoD OIG recommendations, the DSPO issued and implemented the 2015 Strategy for Suicide Prevention to coordinate suicide prevention efforts across the DoD. In response to another OIG report, the DSPO developed and is in the process of issuing guidance for data collection and reporting on suicide events that will also address DoD suicide prevention efforts.

To continue monitoring suicide prevention efforts, the DoD OIG will conduct an evaluation of DoD Suicide Prevention Policy Dissemination and Implementation.

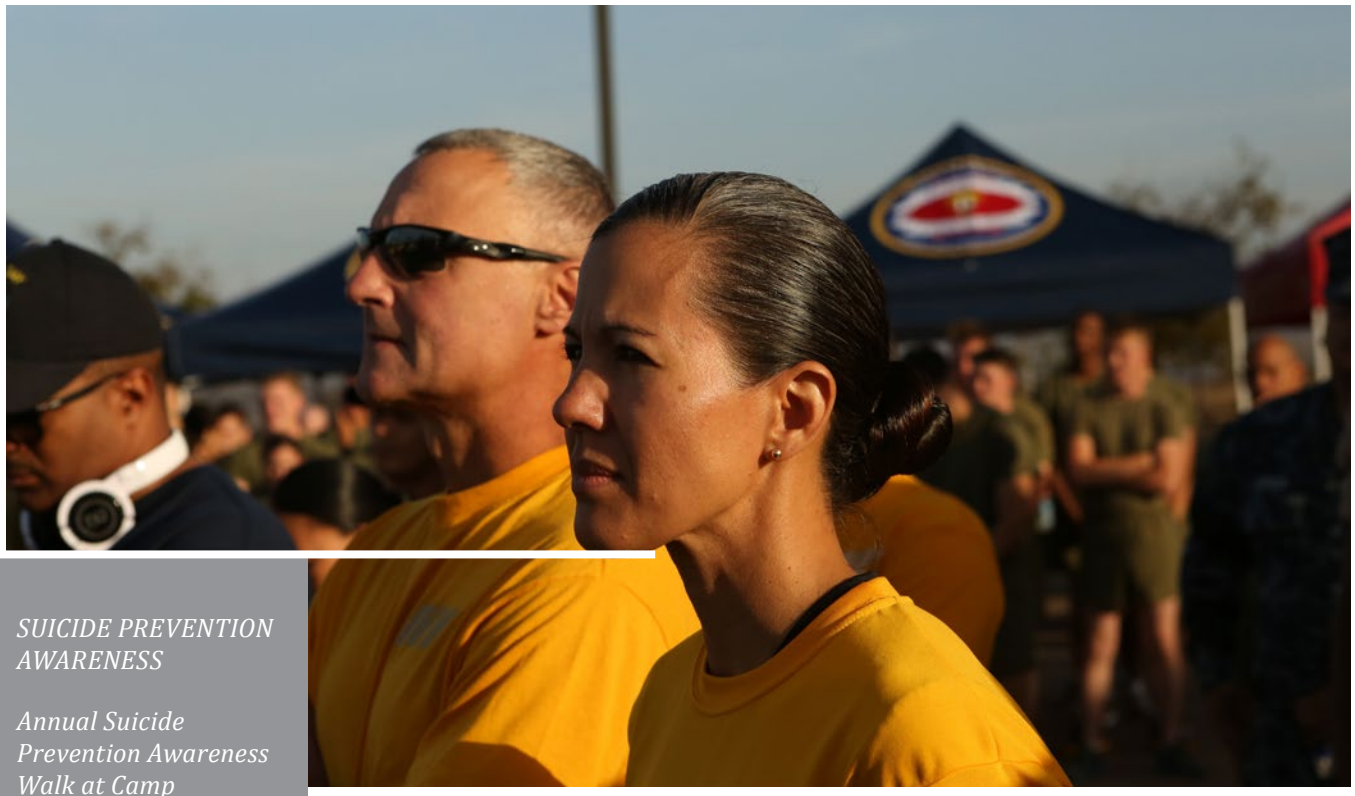
Health Care

Providing quality health care for members of the Military Services and their families remains a challenge that is critical to force readiness. The Military Health System must provide care for over 9 million beneficiaries within fiscal constraints, while facing increased user demand and inflation. These challenges make cost control difficult. Over the last decade, health care costs in the United States have grown substantially, and Military Health System costs have been no exception. The DoD FY 2014 appropriations for health care were $32.7 billion, an increase of about 80 percent since FY 2005. Appropriations have almost tripled since the FY 2001 appropriation of $12.1 billion. In its FY 2017 budget, the DoD requested $33.8 billion for the Defense Health Program.

Over the last decade, health care costs in the United States have grown substantially, and Military Health System costs have been no exception.

The DoD faces additional health care challenges such as preventing health care fraud, containing costs, and ensuring access to quality care. Health care fraud is another one of the top investigative priorities of DCIS. The DCIS has many open health care criminal investigations. As of September 30, 2016, DCIS had 492 open health care cases that represent approximately 30 percent of DCIS's open investigations. In FY 2016, DCIS' health care fraud investigations resulted in 45 criminal charges, 34 convictions, and over $763million in recoveries for the Government. In FY 2016, DCIS' health care fraud cases have resulted in 32 criminal charges, 16 convictions, and over $380 million in recoveries for the Government.

As noted above, the DoD continues to struggle to contain costs in TRICARE programs. As one example affecting the rise in costs, the TRICARE Pharmacy Program experienced a dramatic rise in the receipt and payment of compounded drug prescriptions. Compounding pharmacies combine, mix, or alter two or more ingredients to create a customized medication for



SUICIDE PREVENTION AWARENESS

Annual Suicide Prevention Awareness Walk at Camp Pendleton, CA, is held to increase awareness about suicide and highlight the resources available.

Photo courtesy of U.S. Marine Corps, Lance Cpl. Joseph Sorci

patients. From October 2014 to April 2015, payments for compound drugs increased from $84 million to $550 million per month, or 555 percent over the 7-month period. However, much of the increase was based on fraudulent activity. The DCIS opened 133 investigations relating to fraud by compounding pharmacies, many of which addressed allegations of health care kickbacks between the pharmacies, the marketers of the drugs, and the prescribing physicians. Often, the marketers used "pyramid schemes" to recruit individuals to promote the medications, and they often contacted TRICARE beneficiaries using direct marketing techniques. Frequently there was no doctor-patient relationship between the prescribing physicians and the beneficiaries, which is a requirement to bill under the TRICARE Program. Additionally, the majority of these fraudulent prescriptions were for creams that supposedly treated generic conditions such as pain and scarring.

A joint DCIS and FBI investigation led to the indictments of two individuals associated with a Texas-based company that marked compounded pain and scar creams to TRICARE beneficiaries on behalf of compounding pharmacies. The individuals were indicted on various health care fraud and other charges. The indictment alleged that defendants paid kickbacks of $250 per month to TRICARE beneficiaries for each compounded prescription they obtained, and paid physicians $60 for

each compounded pain or scar cream they prescribed. The loss to TRICARE from their alleged scheme exceeded $65 million. The indictment contains a forfeiture allegation which would require the defendants, upon conviction, to surrender property traceable to the offenses including four homes, 18 bank accounts, and 21 cars and trucks, two motor coaches, and a boat. The investigation remains ongoing. A separate DCIS compounding pharmacy investigation resulted in a company paying the Defense Health Agency approximately $8 million to resolve allegation that it violated the False Claims Act by billing the TRICARE Program for compounded prescriptions that were not medically necessary and were not reimbursable.

While most of DCIS' compounding pharmacy investigations remain ongoing, they have already resulted in 38 criminal charges, four convictions, over $300 Million in seized assets, and over $90 million of recoveries.

In May 2015, the Defense Health Agency implemented new controls to reduce payments for compound drugs from $497 million in April 2015 to approximately $10 million in June 2015. The DoD OIG reported in July 2016 that while the controls were effective in reducing costs for compound drugs, additional controls were necessary to prevent reimbursement for certain non-covered compound drug ingredients. The Defense Health Agency concurred with the recommendation and is taking action to improve controls.

The DoD OIG reported in July 2016 that while the controls were effective in reducing costs for compound drugs, additional controls were necessary to prevent reimbursement for certain non-covered compound drug ingredients.

In addition to controlling health care costs, the DoD should improve collections for services provided at military treatment facilities. The DoD OIG issued five reports from August 2014 through April 2016 and concluded that military treatment facilities did not actively pursue collections from non-DoD beneficiaries for 120 accounts, valued at $11.3 million, of the 125 accounts the DoD OIG reviewed. Also, the military treatment facilities did not appropriately transfer funds to the U.S. Treasury for 114 delinquent accounts, valued at $13.4 million, of the 125 accounts the DoD OIG reviewed for collection.

The DoD OIG is also planning to review whether DoD is adequately meeting quality of care and patient safety standards for DoD service members and beneficiaries.

The DoD must remain competitive in its challenging efforts to recruit, develop, promote, and retain talented and skilled service members and civilians to serve the nation.

Talent Management, Force of the Future

The DoD is the nation's largest employer, with over 1.3 million men and women on active duty, 700,000 civilian personnel, and 800,000 personnel serving in the National Guard and Reserve forces. The DoD must remain competitive in its challenging efforts to recruit, develop, promote, and retain talented and skilled service members and civilians to serve the nation.

One example of this challenge is the reported shortage of Air Force drone and jet pilots. Air Force leadership has testified that the Air Force needs over 500 fighter jet pilots and approximately 500 drone pilots. Air Force leadership further testified that airlines have been recruiting Air Force pilots and that contracting firms have been offering high salaries to drone pilots. The GAO also testified that a series of interviews with drone pilots found low morale and that the pilots believed that a negative stigma was attached to their role. These challenges highlight the importance of talent management within the DoD.

In November 2015, the Secretary of Defense announced an initiative to examine DoD's civilian and military personnel practices. The goal of these efforts is to identify innovative and new ways to revitalize personnel and talent management systems and processes, which address changes in generations, technologies and labor markets. To meet the intent of this initiative, the DoD has identified approaches to modernize DoD personnel policies, procedures, and practices. In January 2016, the Secretary of Defense announced a second set of workforce reforms to improve the retention of service members and encourage public service.

In sum, the DoD continues to struggle in the areas of equipment accountability, suicide prevention, containing health care costs, and recruiting and retaining individuals. The OIG will continue to perform work in these areas in order to monitor the DoD's progress.

GRADUATION

The U.S. Air Force Academy's class of 2015, 800 strong, tosses their hats in celebration. The cadets became second lieutenants upon gradutaion.

Photo courtesy of U.S. Air Force, Liz Copan

the Challenge—#9

Ensuring Ethical Conduct

Public trust and confidence in the DoD can be undermined by the small percentage of individuals who commit misconduct or crimes. High-profile scandals, corruption, waste, abuse of authority, acts of reprisal, or sexual assault involving DoD personnel are contrary to the DoD's high standards of integrity. The DoD must seek to minimize such misconduct and hold accountable anyone who commits it.

The Secretary of Defense and DoD leaders have repeatedly recognized this and stressed the need to make it a priority for the DoD to maintain ethical conduct and a culture in which honesty, accountability, respect, and integrity guide individual actions and decisions.

For example, in a memorandum dated February 12, 2016, "Leader-Led, Values-Based Ethics Engagement," the Secretary of Defense informed the DoD's leaders of his expectations regarding the importance of integrity and public confidence in Defense activities and its people. The Secretary directed that leaders, at every level, engage personally with their subordinates to discuss values-based decision making as set forth in the Joint Ethics Regulation to foster a culture of ethics and promote accountability, respect, and transparency throughout the DoD.

The Secretary directed that leaders, at every level, engage personally with their subordinates to discuss values-based decision making as set forth in the Joint Ethics Regulation to foster...

To pursue this objective, in March 2014 the Secretary of Defense established the position of Senior Advisor for Military Professionalism, which is currently filled by Rear Admiral Margaret "Peg" Klein. The Secretary charged Admiral Klein to work directly with the Service Secretaries and Chiefs regarding the DoD's focus on ethics, character, competence, and accountability in all activities at every level of command. In addition to regularly stressing positive examples of ethical leadership, in February 2016 Admiral Klein led the first DoD Professionalism Summit, which provided military leaders the opportunity to collaborate and share information on values-based leadership, character, and leadership development. The DoD OIG has engaged Admiral Klein and the Service IGs in regular meetings to share information on matters relating to senior official and whistleblower investigations, including the types of substantiated misconduct, outreach and training efforts, and efforts to improve the investigation of misconduct.

In another example of Service-level leadership, in April 2016 the Chief of Naval Operations (CNO) released the personal message he had provided to the Naval Flag officers and Senior Executive Service members emphasizing the Navy's core values of honor, courage, and commitment and the core attributes of integrity, accountability, initiative, and toughness. The CNO emphasized to the Navy senior leaders that their personal conduct, and the example it sets, are essential to their credibility, as well as the overall integrity and efficiency of the Navy.

Investigations of Allegations of Senior Official Misconduct

Addressing misconduct when it occurs is essential to promoting ethical conduct throughout the DoD. It is important to hold individuals accountable if they have committed misconduct or clear individuals who have not. Therefore, investigations of misconduct should be conducted thoroughly and in a timely manner.

WEST POINT

The Class of 2020 conclude Cadet Basic Training with a 12-mile road march.

Photo courtesy of U.S. Army, John Pellino

The DoD OIG and the Military Service IGs have received a large number of complaints and investigations involving allegations of senior official misconduct over the past several years. For example, from FY 2013 through FY 2015, the DoD and Military Service IGs received an average of 792 complaints and conducted an average of 260 investigations involving non-reprisal allegations against senior officials per year. Of those investigations, an average of 79 (30%) were substantiated each year. The types and severity of some of the substantiated misconduct is troubling. For example, recent investigations have substantiated serious misconduct by senior DoD officials such as accepting gifts from a Defense contractor, engaging in inappropriate relationships, and misusing Government resources.

Timeliness of investigations of misconduct remains a challenge. To pursue this objective, the Deputy Secretary of Defense asked the DoD OIG to lead a task force to examine ways to improve the timeliness of senior official investigations throughout the DoD. The DoD OIG teamed with the Military Service IGs and made recommendations to improve timeliness of investigations such as deploying a uniform administrative investigation case tracking system across the DoD, implementing a standardized system of investigative milestones among the Service IGs, providing uniform training for investigators, and monitoring the timeliness of investigations on a regular basis.

Despite these steps, timeliness of investigations remains a challenge throughout the DoD, given the increasing number of cases, the need for addressing allegations fully, and the limited level of resources devoted to these investigations.

Whistleblower Reprisal Investigations

Whistleblowers are important to exposing waste, fraud, and abuse in Government programs, and they are instrumental in saving taxpayers' money and improving the efficiency of Government operations. Whistleblowers must be protected from reprisals for protected disclosures. The DoD OIG is responsible for conducting and overseeing investigations when whistleblowers allege they have suffered reprisal. Without such investigations to protect whistleblowers from reprisal, individuals who can help save taxpayers' money—and possibly even save lives—may not report crucial information about wrongdoing and waste.

The DoD OIG and the Service IGs therefore seek to conduct thorough, fair, and timely investigations into allegations of whistleblower reprisal. It is a challenging task, particularly given the burgeoning whistleblower reprisal caseload and the flat level of resources available for such investigations in the DoD OIG and the Service IGs.

The DoD OIG has implemented improvements to the military whistleblower reprisal investigation program and is seeking to implement others. For example, the DoD OIG is seeking improvements throughout the DoD such as standardizing whistleblower reprisal investigations and implementing a DoD enterprise case management system for tracking administrative investigations.

In addition, in 2016 the DoD OIG established a dedicated team to investigate reprisal complaints stemming from whistleblowers who reported sexual assault. This action implemented one of the recommendations made by the Judicial Proceedings Panel in its "Report on Retaliation Related to Sexual Assault Offenses," which recommended that the DoD OIG investigate all complaints of professional retaliation related to sexual assault and ensure that these investigations are conducted by personnel with specialized training.

The Secretary directed that leaders, at every level, engage personally with their subordinates to discuss values-based decision making as set forth in the Joint Ethics Regulation to foster...

Sexual Assault Prevention and Response

According to the DoD Annual Report on Sexual Assault in the Military Fiscal Year 2015, DoD's prevention programs focus on "reinforcing the cultural imperatives of mutual respect and trust, professional values, and team commitment to create an environment where sexist behaviors, sexual harassment, and sexual assault are not condoned, tolerated, or ignored."

Sexual assaults remain a significant challenge for the DoD. The DoD must focus on reducing sexual assaults and protect those who report sexual assaults from retaliation. According to the DoD Annual Report on Sexual Assault in the Military Fiscal Year 2015 issued on May 2, 2016, DoD's prevention programs focus on "reinforcing the cultural imperatives of mutual respect and trust, professional values, and team commitment to create an environment where sexist behaviors, sexual harassment, and sexual assault are not condoned, tolerated, or ignored." This report indicated that the DoD is working to address six key areas: 1) Advancing sexual assault prevention; 2) Encouraging greater reporting of sexual assaults; 3) Encouraging the reporting of sexual harassment complaints; 4) Improving response to male victims; 5) Combatting retaliation associated with sexual assault reporting; and 6) Tracking accountability in the military justice system.

According to the DoD annual report, fewer sexual assaults occurred in the military in 2014 than in 2006 when the DoD Sexual Assault Prevention and Response Program began, but a greater percentage of victims reported the crime. The DoD attributes changes in reporting behavior in part to the growth in sexual assault prevention and response programs since 2006. The annual report also stated that more must be done to implement an enduring culture change to enable service members to operate in a climate without sexual assault, including:

- creating the 2017–2021 Sexual Assault Prevention Plan of Action to advance the effectiveness of military sexual assault prevention programming; and
- launching the DoD Prevention Collaboration Forum to initiate greater coordination with other DoD programs that address readiness impacting problems to leverage a unified approach to prevention—these programs include Family Advocacy Program, Defense Suicide Prevention Office, and the Office of Diversity Management and Equal Opportunity.

With respect to oversight of investigations of sexual assault allegations, the DoD OIG has a unit staffed with criminal investigators to oversee the DoD's sexual assault investigations. The DoD OIG also implemented overarching sexual assault investigative policy guidance to ensure uniform reporting and DoD investigations of sexual assaults. Since then, DoD policies have been updated to remain current of new legislative

CAPITAL SHIELD 2016

Army Reserve and active duty agents participate in a joint training exercise focusing on crive scene processing, evidence management and hostage negotiations.

Photo courtesy of U.S. Army Reserve, Master Sgt. Michel Sauret

requirements, including the establishment of Special Victim Investigation Program implementing guidance for the investigation of all unrestricted reports of sexual assault with adult victims, crimes with child victims, and reports of domestic violence.

Nevertheless, preventing sexual assaults, ensuring victims who report sexual assault do not suffer retaliation, and fully investigating allegations in a timely manner remain a continuing challenge throughout the DoD.

Public Corruption Investigations

Public Corruption involving the DoD and its personnel and programs wastes billions of tax dollars and can undermine public trust in the DoD. Yet, criminal misconduct by Government and contractor personnel in the DoD continues to pose a management challenge. The DCIS considers public corruption investigations to be among its highest priorities. In FY 2015, DCIS's public corruption investigations led to 52 criminal charges, 52 criminal convictions, and over $18 million in restitution and other monetary recoveries payable to the Government. The data for DCIS's work for FY 2016 is expected to be comparable.

The DoD needs to remain focused on ensuring ethical conduct and providing necessary resources and support for investigations to hold accountable those who do not uphold the high standards of the DoD.

A particularly compelling example of public corruption in DoD programs involves a decades-long conspiracy of bribery and fraud by Glenn Defense Marine Asia PTE, LTD (GDMA). The investigation is ongoing and is being conducted jointly by DCIS and the Naval Criminal Investigative Service. The scheme involved the routine overbilling for goods and services that GDMA provided to Navy ships at various Asian seaports, including fuel, tugboat services, and sewage disposal. As of October 1, 2016, 15 individuals have been charged in connection with this scheme. A total of 11 of those individuals have pleaded guilty, including a Navy Rear Admiral, a Navy Captain, several other Navy officers and enlisted personnel, a NCIS special agent, GDMA's president, a former GDMA employee, and the GDMA corporate entity.

In summary, ensuring ethical conduct must be the focus of continual attention. The creation of a position such as the Senior Advisor for Military Professionalism to addresses ethical matters, and the emphasis placed on improving programs to prevent and investigate sexual assaults, demonstrate commitment at DoD's highest levels to address this challenge. However, an organization the size of the DoD will inevitably be faced with waste, fraud, abuse, assaults, and ethical misconduct by some employees and contractors. The DoD needs to remain focused on ensuring ethical conduct and providing necessary resources and support for investigations to hold accountable those who do not uphold the high standards of the DoD.

AIR FORCE ONE

Saluting Air Force One as it prepares for departure from Joint Base Andrews, Md.

Photo courtesy of Air Force Senior Master Sgt. Kevin Wallace/Released

the Challenge—#10

Promoting Continuity and Effective Transistion Management

Changes of Presidential Administrations typically bring widespread turnover in DoD leadership positions as political appointees depart and potential delays occur in filling those vacancies. According to the most recent edition of the Plum Book, in 2012 the DoD had 54 Presidentially Appointed, Senate-confirmed positions and 544 non-Presidentially Appointed Senate-confirmed positions potentially filled by political appointees.

SENATE CONFIRMATION

West Front of the U.S. Capitol Building, Washington D.C.

Photo courtesy of istockphoto

While managing Presidential transitions is a challenging issue for all Federal departments and agencies, it is especially true for the DoD because of the national security implications. The importance of effectively managing the transition to a new administration is heightened now with the DoD engaged in two overseas contingency operations (OIR and OFS) and countering the evolving threats around the world. Gaps in leadership, delays in approving key decisions, and uncertainty about policy objectives can have significant effects on national security. For that reason, it is critical that the transition to new leadership be smooth, effective, timely, and seamless.

Moreover, on a regular basis, changes of leadership at all levels occur frequently throughout the DoD. Senior military leaders rotate positions every 1 to 3 years, as do military leaders at junior levels and forward deployed forces. This also presents a challenge for the DoD in ensuring continuity of operations.

Presidential Appointments

Expediting the appointment of incoming senior leaders within DoD is critical to the efficient and effective transfer of responsibility.

Expediting the appointment of incoming senior leaders within DoD is critical to the efficient and effective transfer of responsibility. During vacancies in leadership positions, career officials in acting positions are often responsible for managing their organizations. These officials are not able to make significant program or operational changes within their components.

In addition, comprehensive and accurate reporting on DoD programs, operations, and challenges is an important element for ensuring efficient and effective policy implementation by the incoming administration. DoD Components must be prepared to provide the incoming presidential transition staff with necessary briefings to assist in the identification of component-specific policy or program initiatives and challenges that require immediate attention. These comprehensive briefings should continue whenever new leadership arrives at the DoD.

Operations

Access to DoD facilities and information, facilitation of communication between DoD and presidential transition organizations, and the provision of logistics support to the incoming administration are also vital elements to achieving a successful Presidential transition. Focus needs to be given to areas such as access to information technology resources, full briefings on critical areas, and rapid processing of security clearances.

DoD leaders are focusing of transition planning. The Head of DoD Transition has been identified and the DoD Transition Task Force has been created and is meeting regularly to advance transition planning. As part of this effort, the DoD has already begun preparing a transition book and briefing materials for the transition teams and the new administration. The DoD transition book provides a high-level overview of each of the Defense agencies and Components. The book includes briefs on the functions, missions, structure, short and longer term deliverables, current budgets, and manpower.

The DoD OIG is also preparing a separate transition briefing book to provide a more in-depth view of the OIG organization and the work being conducted by our auditors, investigators, and evaluators.

Regular rotation of military leadership in the DoD is a well-established concept. Regular rotations expand an individual's functional, cross-functional, and leadership experience. Rotations also provide opportunities for military personnel to obtain depth and breadth of knowledge, broader perspective of the DoD's mission, and professional enhancement. However, these rotations result in frequent turnover for both senior and junior military leaders throughout the DoD and require careful planning and transition procedures. For example, requiring a strong management internal control plan, as well as documented processes and procedures, can ease these transitions and ensure minimal mission impact. Turnover is a perpetual challenge for the DoD, separate and apart from the significant turnover that accompanies a change of Presidential Administration.

Requiring a strong management internal control plan, as well as documented processes and procedures, can ease these transitions and ensure minimal mission impact.

In sum, the DoD must provide the new administration and its leadership, as well as the new officers that assume their roles during the frequent changes in leadership in the military ranks, with the knowledge and tools necessary to begin the work of leadership throughout DoD as soon as possible without gaps or delays.

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

For Report Notifications
www.dodig.mil/pubs/email_update.cfm

Twitter
https://twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098